Immigration, Refugees and Citizenship Canada
Immigration, Réfugiés et Citoyenneté Canada

Assistant Deputy Minister Operations
Sous-ministre adjoint Opérations

Ottawa K1A 1L1

F-1112641

PROTECTED A

MEMORANDUM TO THE DEPUTY MINISTER AND THE ASSOCIATE DEPUTY MINISTER

TREASURY BOARD POLICY ON SERVICE AND DIGITAL

FOR INFORMATION

SUMMARY

- The purpose of this memorandum is to provide you with information on the requirements of the Treasury Board's Policy on Service and Digital, which came into effect on April 1, 2020. Departments have one year to become compliant with the Policy's requirements.

- The new Policy articulates how Government of Canada organisations should manage service delivery, information and data, information technology and cybersecurity in the digital era.

- Deputy heads are responsible for establishing appropriate governance to ensure the integrated management of these areas. This includes designating officials responsible for leading the departmental service management function and the cybersecurity management function.

BACKGROUND:

- The Policy on Service and Digital and the Directive on Service and Digital were approved in July 2019, with an effective date of April 1, 2020. These Treasury Board policy instruments integrate, streamline and strengthen requirements for managing service, information, data, information technology, and cybersecurity.

- The expected outcome of the Policy is that government operates, designs and delivers client-centric services using digital methods and tools. Over the long term, digital transformation is expected to continually improve the government's operations, services and client experience.

- More specific outcomes that departments are expected to achieve can be found in the Policy on Service and Digital Logic Model (see Annex A).

- Departments have until April 1, 2021, to become compliant with Policy requirements.

Canada

CURRENT STATUS:

- A central tenet of the Policy is the integration of governance, planning, and reporting to support decision-making in service, information, data, information technology and cybersecurity at both a government-wide level and within each Department.

- The Policy serves as an umbrella for a number of supporting tools, including the Directive on Automated Decision-making, which will impose new requirements on Departments related to transparency, accountability, legality and procedural fairness.

- To provide the leadership necessary to operate effectively in the digital era, new policy requirements for deputy heads include:
  - the establishment of integrated departmental governance;
  - the establishment of integrated departmental planning and reporting; and
  - the designation of officials responsible for leading the departmental service management function and the cybersecurity management function.

- The Treasury Board Secretariat (TBS) released a draft Guideline on Service and Digital to accompany the new Policy. It describes specific requirements for Departments, deputy heads and for each functional area: service, information, data, information technology and cybersecurity (linked in Annex B). This guideline will be evergreen.

Governance:

- At the government-wide level, a deputy-level committee will be established to provide advice and recommendations to the Secretary of the Treasury Board and the Chief Information Officer (CIO) of Canada on strategic decisions regarding managing external and internal enterprise services, information, data, information technology and cybersecurity and prioritizing Government of Canada demand for information technology shared services and assets.

- At the departmental level, deputy heads are responsible for establishing the appropriate governance within their Departments to ensure the efficient and effective integrated management of service, information, data, information technology, and cybersecurity. Deputy heads may consider leveraging existing bodies, either by integrating them or making clearer linkages between them, as long as their governance structure allows decision-making to be aligned with other areas of management such as integrated planning and digital enablement.

- Immigration, Refugees and Citizenship Canada (IRCC) readiness: IRCC's current corporate committee structure will be reviewed and revised as needed to ensure that it is well-positioned to meet these new requirements. Any required changes to committee Terms of Reference will be led by Corporate Secretariat.

Integrated Departmental Planning and Reporting:

- Deputy heads are responsible for approving a forward-looking three-year departmental plan for the integrated management of service, information, data, information technology, and cybersecurity. This plan should be issued annually to cover the next three years and is expected to be informed by subject-specific plans.

- It is expected that the TBS will assess Departments' progress on implementing the Policy during the next Management Accountability Framework process, launching in September 2020.

- IRCC readiness: IRCC requires additional internal coordination to meet this requirement, as subject-specific plans have not yet been aligned into one integrated plan. This integration is being led by Transformation and Digital Strategy Sector (TDSS).

Designated Departmental Officials:

- The Policy requires deputy heads to designate a departmental CIO, responsible to lead departmental information technology, information, and data management functions. This is not a new requirement and Zaina Sovani is the current departmental CIO; however, the Policy requires that deputy heads consult with the CIO of Canada prior to appointing, or re-appointing, the departmental CIO position.

- As IRCC has recently established the Chief Data Officer (CDO) organization, it will work in close collaboration with the CIO to ensure that all data requirements of the policy are met.

- For the first time, the Policy requires deputy heads to identify official(s) responsible for leading the service management function, and for leading the cybersecurity management function. Deputy heads may assign these responsibilities at the level they deem appropriate, including assigning responsibility for more than one functional area to a single official. The Policy requires that the CIO and the official(s) responsible for the service management function have direct access to the deputy head.

- Designated officials are expected to provide clarity regarding their roles and related accountabilities to the functional community they serve, to collectively support the deputy head in advancing Government of Canada priorities, and to ensure that their responsibilities are fulfilled in a timely way throughout the planning, decision-making and design processes of a digital organization.

- IRCC readiness: Assistant Deputy Ministers will return to you with options for designating departmental officials on service and cybersecurity.

Other Policy Highlights

Service Management Function:

- Deputy heads are responsible for ensuring the development and delivery of client-centric service by design, including access, inclusion, accessibility, security, privacy, simplicity, and choice of official language. This is a new requirement and will require IRCC to reexamine its service and system design processes to ensure that all elements are considered in the design stages.

- Policy requirements on service, which previously applied only to priority services (see Annex B), will now apply to all IRCC services (approximately 80). This represents a significant increase in scope.

- The designated official for service will be responsible for ensuring that client feedback is collected and used to improve services. IRCC is already well-positioned to meet this requirement, but further improvements in how we collect, share, and analyze client data are also planned to support this deliverable.

Information Technology Management Function:

- The Policy requires the departmental CIO to provide direction to the Department on the management of information, technology, architecture and cybersecurity. This is not a new requirement and the Digital Strategy Branch was created in 2019, in part to respond to this Departmental leadership requirement.

- To aid in meeting this requirement, the CIO established an intake process, creating visibility into the demand for services and the opportunity to align all identified elements at the design stage. In addition, the creation of the Digital Platform Modernization Program, Departmental Enterprise Architecture Board as part of initiative governance ensures that enterprise level considerations for architecture direction, information and data management, cybersecurity, access, privacy, inclusion, accessibility and client-centric service are assessed prior to initiative execution.

- The Policy specifies enterprise-wide requirements for the management of digital identities credentials and access. The previous requirement was for digital identity to be managed at the program level. Within IRCC, the Admissibility Branch in the Strategic and Program Policy (SPP) Sector is leading discussions on an identity strategy, which will meet Departmental objectives, as well as the Policy on Service and Digital objectives.

Information and Data Management Function:

- The Policy requires the departmental CIO to provide direction to the Department and ensure that methodologies, mechanisms and tools are implemented to support the information and data management life cycle – reducing redundancies and enabling interoperability. With the recent creation of the CDO position and the establishment of its role in co-chairing the Departmental Enterprise Architecture Board with TDSS, IRCC is well positioned to address the information and data management requirements of this policy.

- The CDO will be responsible for the establishment of departmental data standards and governance and will work to ensure that these standards are aligned with the activities of the CIO.

- The CDO Council, which is made up of representatives from various Departments including IRCC, has asked TBS to recognize the role of the CDO in the governance of data. The guidelines for the Policy on Service and Digital do not currently recognize the existence of

CDOs outside of CIO organizations, which may lead to confusion about the roles that each should play in the implementation of this policy. However, deputy heads are given the flexibility to assign roles and responsibilities according to the makeup of their respective Departments. IRCC's CDO will continue to clarify its roles and responsibilities within the Department.

Cybersecurity Management Function:

- The Policy states that cybersecurity must be managed at the enterprise level. This requirement is not new, but is a change from the previous direction which required cybersecurity oversight at the initiative level.

- In 2019 the CIO established two areas responsible for cybersecurity oversight; Digital Strategy Branch for strategic direction and oversight, and Information Technology Operations for enterprise-wide operational cybersecurity management.

COMMUNICATIONS IMPLICATIONS:

Internal Communications:

- Communications will work with program branches to determine the best approach to communicate specific activities coming out of the Policy as they come into effect in the future (i.e., communicating to all staff about the designation of the officials to lead the departmental service management function and cyber security service management function or other outcomes affecting all IRCC staff).

- For the present time, as this change in policy impacts specific groups within the Department, targeted direct messaging from the Assistant Deputy Minister of TDSS is recommended to share the requirements of the TBS Policy, as opposed to mass communication.

- The intranet (Connexion) will be updated to reflect the new Policy, where applicable.

Strategic Communications (external):

- Since the requirements of the Policy are administrative in nature at this time, public interest is not anticipated. The three year Departmental plan is an internal planning document and will not be posted or referenced in the public domain.

- A responsive external communications approach is recommended at this time. Media calls will be handled on a case-by-case basis.

NEXT STEPS:

- Departmental stakeholders will work closely together to meet the new Policy requirements.

- A number of key ExCom discussions will be required to implement the Policy, including:

Summer 2020:

- The CDO Branch, within the SPP Sector, will be discussing the role of the CDO and the implementation of the IRCC Data Strategy. This discussion will help clarify the role of the CDO with respect to the implementation of the new Policy on Service and Digital.

- The Digital Strategy Branch in TDSS, in collaboration with Client Experience Branch in Operations Sector, will bring a proposal to ExCom for how IRCC will participate in the establishment of Government of Canada governance and reporting expectations for the new Policy on Service and Digital.

- The CDO is currently establishing an implementation plan for key elements of the IRCC Data Strategy. The CDO will work in collaboration with the Digital Strategy Branch to bring a proposed approach to ExCom, which will describe how the Department will align the Data Strategy with data management requirements of the Policy on Service and Digital.

Fall 2020:

- The Projects Branch in TDSS will bring a proposal to ExCom regarding an approach that will ensure alignment of initiatives to the need for client service, digitization, access, inclusion, accessibility, security, privacy, data, simplicity, and choice of official language.

Winter 2021:

- The Digital Strategy Branch in TDSS, in collaboration with other branches accountable for requirements under the Policy, will bring a forward-looking three-year departmental plan for the integrated management of service, information, data, IT, and cybersecurity, including an approach to digital enablement of all services to ExCom for approval.

e-approved
Zaina Sovani

e-approved
Natasha Kim

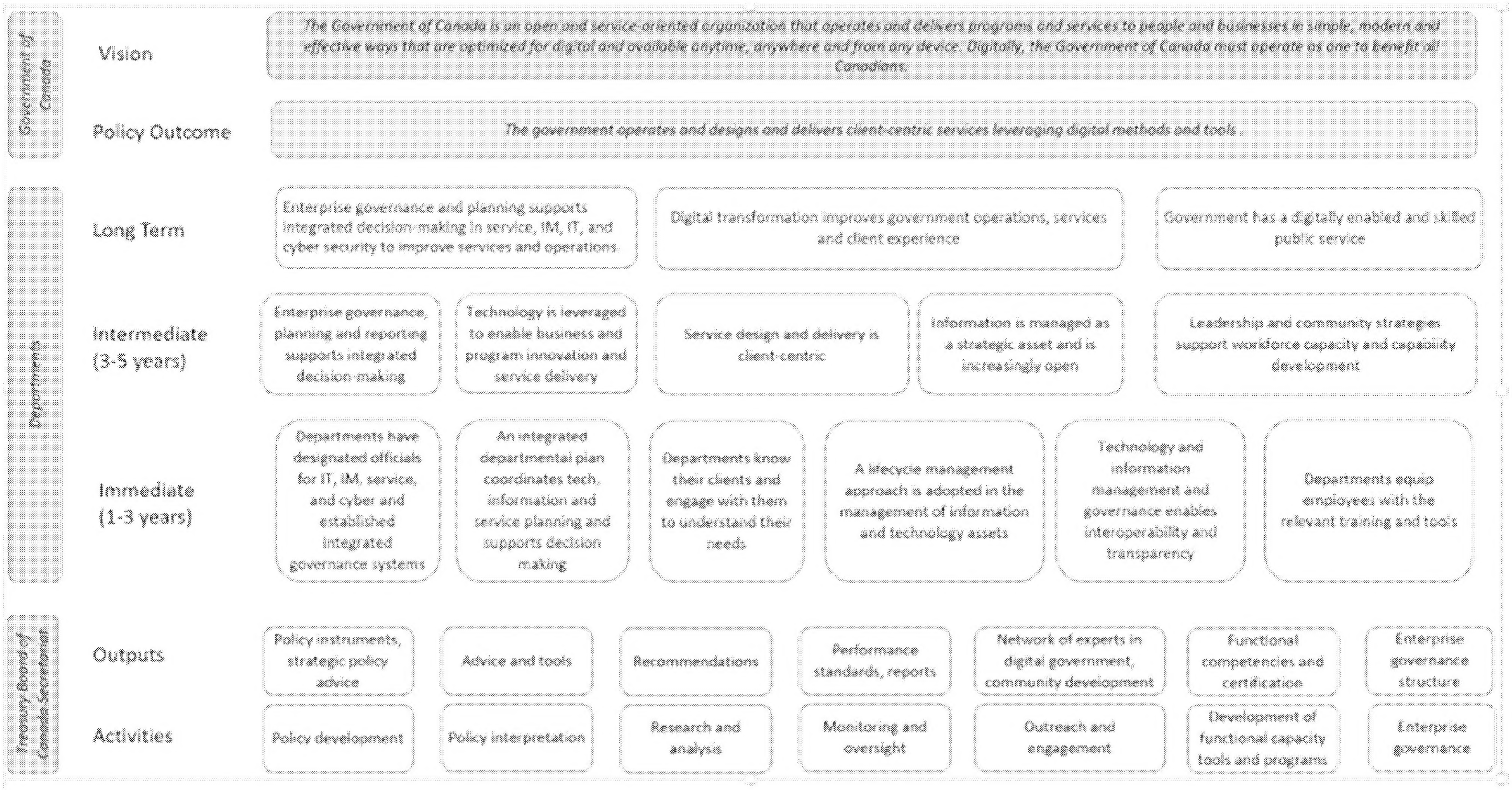
e-approved
Fraser Valentine

e-approved
Daniel Mills

Annexes (2):
A: Policy on Service and Digital Logic Model
B: Link to Draft Guide on Service and Digital

Annex A: *Policy on Service and Digital* Logic Model

The logic model provides a list of outcomes that departments are expected to achieve by implementing the requirements of the *Policy on Service and Digital*.



Government of Canada

Vision

The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device. Digitally, the Government of Canada must operate as one to benefit all Canadians.

Policy Outcome

The government operates and designs and delivers client-centric services leveraging digital methods and tools .

Departments

Long Term

- Enterprise governance and planning supports integrated decision-making in service, IM, IT, and cyber security to improve services and operations.
- Digital transformation improves government operations, services and client experience
- Government has a digitally enabled and skilled public service

Intermediate (3-5 years)

- Enterprise governance, planning and reporting supports integrated decision-making
- Technology is leveraged to enable business and program innovation and service delivery
- Service design and delivery is client-centric
- Information is managed as a strategic asset and is increasingly open
- Leadership and community strategies support workforce capacity and capability development

Immediate (1-3 years)

- Departments have designated officials for IT, IM, service, and cyber and established integrated governance systems
- An integrated departmental plan coordinates tech, information and service planning and supports decision making
- Departments know their clients and engage with them to understand their needs
- A lifecycle management approach is adopted in the management of information and technology assets
- Technology and information management and governance enables interoperability and transparency
- Departments equip employees with the relevant training and tools

Treasury Board of Canada Secretariat

Outputs	Policy instruments, strategic policy advice	Advice and tools	Recommendations	Performance standards, reports	Network of experts in digital government, community development	Functional competencies and certification	Enterprise governance structure
Activities	Policy development	Policy interpretation	Research and analysis	Monitoring and oversight	Outreach and engagement	Development of functional capacity tools and programs	Enterprise governance

The outcomes shown in the logic model will be further articulated in future guidance and tools to support departments from a performance measurement perspective in their transition toward a digital government.

Source: Pg 134 Draft Guide on Service and Digital v1.1 - TBS

Guideline on Service and Digital

About this guideline

This *Guideline on Service and Digital* supports the Treasury Board *Policy on Service and Digital* and *Directive on Service and Digital*. It provides interpretative guidance related to the requirements associated with managing service, information, data, IT and cyber security.

Although this guideline is primarily for Government of Canada organizations to which the policy applies (see subsection 6 of the *Policy on Service and Digital*), all federal departments and agencies[1] are encouraged to follow the advice provided, as appropriate.

This guideline was prepared by the Office of the Chief Information Officer of the Treasury Board of Canada Secretariat (TBS), and was informed by feedback received from departments and other stakeholders.

The guideline has five sections that mirror the structure of the policy and directive. In each section, the requirements of the policy and directive are grouped into themes. For each theme, the guideline provides information about:

- what the theme means
- why the theme is important
- considerations in implementing the associated requirements of the policy and directive

Although this guideline aims to be comprehensive, it does not provide specific guidance on fulfilling each requirement of the policy and directive. Additional guidance and tools will be developed in collaboration with departments and other stakeholders to address any gaps and further support implementation.

[1] Throughout this guideline, federal departments and agencies are referred to as departments.

Document control

Document version	**Release date**
Draft release (version 1.0)	January 22, 2020

Introduction

The *Policy on Service and Digital* and the *Directive on Service and Digital* were approved in July 2019, with an effective date of April 1, 2020. These Treasury Board policy instruments have been developed through extensive engagement and collaboration with departments and other stakeholders.

The policy and directive integrate, streamline and strengthen requirements for managing the following functional areas:

- service
- information
- data
- information technology (IT)
- cyber security

The expected outcome of the policy is that government operates, designs and delivers client-centric services using digital methods and tools. Over the long term, digital transformation is expected to continually improve the government's operations, services and client experience. Refer to Appendix A of this guideline lists the outcomes that departments are expected to achieve by fulfilling the requirements of the policy and the directive.

The requirements set out in the policy and the directive are guided by the overarching principles and best practices known as the Government of Canada Digital Standards:

- design with users
- iterate and improve frequently
- work in the open by default
- use open standards and solutions
- address security and privacy risks
- build in accessible from the start
- empower staff to deliver better services
- be good data stewards
- design ethical services
- collaborate widely

The policy must also be applied in conjunction with other policies and legislation, including in the areas of privacy, security, official languages and accessibility (see section 8 of the *Policy on Service and Digital*).

1. Integrated governance, planning and reporting

Good governance is essential in improving the Government of Canada's operations and services. Governance establishes how the government exercises authority, accountability, leadership, direction and control.

Among the expected outcomes of the *Policy on Service and Digital* is the integration of governance, planning and reporting, government-wide and at each department, to support integrated decision-making in service, information, data, IT and cyber security. Integration also ensures that considerations for each function is included at the outset.

1.1 Integrated governance

1.1.1 Description and associated requirements

Integrated governance means that all pertinent officials are brought together at the decision-making table, government-wide and at departments. More specifically, it means that officials responsible for service design and delivery, information, data, technology and cyber security are engaged at the outset so that considerations related to their respective areas of expertise are reflected at all stages.

At the government-wide level, a deputy-level committee will be established to provide advice and recommendations to the Secretary of the Treasury Board and the Chief Information Officer (CIO) of Canada on strategic decisions regarding:

- managing external and internal enterprise services, information, data, IT and cyber security
- prioritizing Government of Canada demand for IT shared services and assets

The CIO of Canada is responsible for providing advice to the Secretary on these matters, as outlined in the following requirements:

Requirements for the Treasury Board of Canada Secretariat (TBS) under the policy

The **Secretary of the Treasury Board of Canada** is responsible for:

4.1.1.1 Establishing and chairing a senior-level body that is responsible for providing advice and recommendations, in support of the Government of Canada's priorities and the Government of Canada Digital Standards, regarding:

4.1.1.1.1 Strategic direction for the management of external and internal enterprise services, information, data, information technology (IT) and cyber security; and

4.1.1.1.2 Prioritization of Government of Canada demand for IT shared services and assets

The **Chief Information Officer (CIO) of Canada** is responsible for:

4.1.2.1 Providing advice to the Secretary of the Treasury Board of Canada and the President of the Treasury Board of Canada about:

4.1.2.1.1 Governing and managing enterprise-wide information, data, IT, cyber security, and service design and delivery;

4.1.2.1.2 Prioritizing Government of Canada demand for IT shared services and assets; and,

4.1.2.1.3 Using emerging technologies and the implications and opportunities of doing so for the Government of Canada.

Requirements for the Treasury Board of Canada Secretariat (TBS) under the policy	
4.1.2.2	Providing direction on the enterprise-wide transition to digital government, including: regularly reviewing and updating the Government of Canada Digital Standards; managing information, data, IT, and cyber security; and, advising on enterprise-wide service design and delivery.
4.1.2.5	Establishing priorities for IT investments (including cyber security investments) that are enterprise-wide in nature or that require the support of Shared Services Canada (SSC).

At the departmental level, deputy heads are required to establish integrated departmental governance to ensure the efficient and effective integrated management of these functions within their organizations.

Requirement for departments under the policy	
Deputy heads are responsible for:	
4.1.3.1	Establishing governance to ensure the integrated management of service, information, data, IT, and cyber security within their department.

1.1.2 Why is this important?

Effective governance is one of the foundational enablers to becoming an open and digital government. Supporting the implementation of a government-wide approach to digital requires integrated discussions so that the focus is on:

- business needs, including improving services to clients
- ensuring the sustainability of technology (for example, replacing legacy systems)

Too often, implementing technology has not sufficiently considered clients' needs. It is important that the governance model for service and digital integrates and aligns the five principal functions (service, information, data, IT and cyber security).

Integrated governance can enhance organizations' ability to make decisions strategically at the outset. Specifically, establishing governance that integrates how service, information, data, technology and cyber security are managed has several benefits:

- services become digitally enabled
- linkages can be made across areas of management
- activities in each area of management are aligned with clear business outcomes (for example, service, operations)

- aspects related to service design and delivery, information, data, technology and cyber security, as well as horizontal considerations such as privacy protection, are addressed proactively at the outset
- a holistic approach prevents blind spots and unnecessary risks associated with working in silos
- decision-makers can have a horizontal view and identify issues earlier in the process to enable course correction, pausing or halting as needed
- discussions about initiatives to obtain all relevant perspectives can occur in one forum
- various areas of management are closer to where decisions are made and are better able to inform decision-making in a timely way
- CIOs and other officials become strategic business partners

1.1.3 Considerations in implementing the requirements

There are a few considerations that departments may want to take into account when "establishing governance to ensure the integrated management of service, information, data, IT, and cyber security within their department" (*Policy on Service and Digital*, subsection 4.1.3.1):

- There are various ways that departments can integrate governance within their organizations. Governance structures vary depending on a department's size, mandate, sector and nature of work. In establishing governance, deputy heads may consider leveraging existing bodies, either by integrating them or making clearer linkages between them, as long as their governance structure allows decision-making to be carried out in a way that is integrated with other areas of management.
- The scope of integrated governance, as required by the policy, should address how departments manage service, information, data, IT and cyber security. The scope should correspond with the terms of reference of the government-wide committee on governance and could include direction to the organization's deputy head on:
    - horizontal trends and issues that affect departmental service delivery and operations, to better support individuals' and businesses' access to services that are client-centric, trusted and secure
    - horizontal strategic and operational uses of information and data within the organization, consistent with privacy requirements and following government-wide direction
    - horizontal strategic and operational uses of IT (including cyber security considerations) within the organization, following government-wide standards and direction
- Although there is no formal reporting relationship between departmental governance and the enterprise governance committee, a department's deputy head may bring forward issues discussed departmentally to the committee, when appropriate. Such discussion can promote government-wide efficiencies.

- Given that service and business needs drive enabling technology and strategic management of information and data, departments could consider linking decisions made on technology, information, data and cyber security to a clear business outcome and improved service. In addition, other considerations such as privacy and accessibility should be integrated into digital service design from the outset.
- Although the main focus is on specific areas of management, other important horizontal considerations could be raised and addressed through governance discussions, such as openness, inclusion, accessibility, security, privacy, simplicity and choice of official language, as mentioned in other requirements of the policy. Departmental leads for other related areas, such as privacy, open government and accessibility, should be included in these discussions.

1.2 Designation of officials

1.2.1 Description and associated requirements

To support more integrated governance and leadership necessary to operate effectively in the digital era, requirements in the policy include the designation of the following:

- an official responsible for leading the departmental service management function
- a departmental CIO
- an official responsible for leading the cyber security management function

Designated these officials will ensure clarity in their roles and accountabilities to the functional community they serve. The policy requires that the official responsible for the service management function and the departmental CIO have direct access to the deputy head.

Requirements for departments under the policy
Deputy heads are responsible for: 4.1.3.2 Designating a departmental CIO responsible for leading the departmental IT, information, and data management functions. 4.1.3.3 Designating an official responsible for leading the departmental service management function. 4.1.3.4 Designating an official responsible for leading the departmental cyber security management function. 4.1.3.5 Providing the departmental CIO and the official responsible for service with direct access to the deputy head. 4.5.2.3 Consulting with the CIO of Canada before appointing, deploying, or otherwise replacing the departmental CIO.

1.2.2 Why is this important?

Because the government is increasing its focus on clients' needs, departmental officials must be designated specific roles in order to ensure focus and support. Establishing a specific role for cyber security is also important, as the government is increasingly relying on digital technologies for its operations and services.

Within departments, these officials:

- collectively support the deputy head in advancing functional areas
- ensure that their responsibilities are fulfilled in a timely way throughout the planning, decision-making and design processes of a digital organization

The benefits of designating officials for functional areas include the following:

- a coordinated and strategic approach to management that is at the departmental level that supports deputy heads, with better advice on how the functional areas can help support departmental priorities that align with the Government of Canada direction
- enhanced clarity in roles and related accountabilities for each functional area
- a centralized perspective that allows for efficiencies across departmental program areas
- increased linkages with other supporting functions across the department (service, IT, information, data, cyber security, privacy) that can improve services and operations while meeting privacy, security and other obligations

1.2.3 Considerations in implementing the requirements

The policy gives deputy heads the flexibility to determine who should be responsible for service management, cyber security and CIO functions. Deputy heads may assign these responsibilities at the level they deem appropriate, including assigning responsibility for more than one functional area to a single official. Deputy heads may also establish other senior roles, such as chief data officer, if they deem it necessary.

Although these officials are responsible for their own functional areas, it is expected that linkages be made with other functional communities (such as privacy protection) across the department to improve the department's services and operations. Integrated governance is one way to support these linkages and collaboration between functional areas (see subsection 1.1 of this guideline).

The policy requires that the departmental CIO and the official responsible for service have direct access to the deputy head. Such access can be implemented in various ways at different departments and may vary based on considerations such as the department's size and mandate. Although the deputy head has discretion in deciding how to establish the reporting structure within the department, it is recommended that the department's CIO and the official responsible for service report directly to the deputy head, with a seat at the executive table. However, because departments can have such different organizational structures, other ways to provide direct access could be through any of the following:

- the official reports directly to the deputy head
- the official has regular bilateral or multilateral meetings with the deputy head
- the official is a member of the executive committee or other governance committee chaired by the deputy head
- the official communicates directly with the deputy head as needed

Considerations for designating an official responsible for leading a department's service management function

The role for the official responsible for leading a department's service management function could include the following:

- promoting a centralized perspective on service, allowing for improved efficiencies in the department's policy and program areas
- providing leadership on managing service, including coordinating department-wide activities related to service, including:
    - governance
    - planning and performance measurement activities
    - service inventory
    - service standards
    - service review
    - client feedback
- supporting the deputy head in fulfilling departmental priorities
- collaborating with central agencies and other departments on government-wide priorities and strategies for service, including keeping current on:
    - administrative policy requirements and other TBS direction
    - activities that stem from the service functional community
- ensuring that:
    - other functions (IT, information, data, cyber security, privacy protection) are leveraged
    - linkages are made to ensure a holistic approach to improving how service design and delivery are managed throughout the department

A deputy head should take special care when considering designating someone as both the chief financial officer and the official responsible for leading the department's service management function. Subsection 4.1.10 of the *Policy on Financial Management* stipulates that chief financial officers cannot be assigned non-financial corporate responsibilities that could compromise their objectivity.

In designating an official responsible for a department's service management function, deputy heads can consider the following competencies:

- leadership competencies
- knowledge of departmental and government-wide governance frameworks (knowing the key partners and knowing where to go and when to go)
- knowledge of departmental and government-wide services
- familiarity with the service direction of the Government of Canada (that is, its priorities and strategies)
- familiarity with Treasury Board administrative policy requirements related to service (the *Policy on Service and Digital* and related policy instruments)
- knowledge of government obligations regarding IT, information, data, security, cyber security and privacy and how these relate to service
- knowledge of the department's clients and their needs and expectations
- the ability, to collaborate and communicate
- knowledge of strategic planning and performance measurement

Considerations for designating a CIO responsible for leading a department's IT, information and data management functions

Departmental CIOs remain responsible for managing information and IT, and they are to be involved throughout the life cycle of how services are designed and delivered in order to continually improve how client's needs are met. In addition to fulfilling the requirements set out in the *Directive on Service and Digital*, the CIO is responsible for the following:

- managing departmental information, data and IT
- being a strategic voice at the executive table who advises on digitally enabled approaches to meet departmental and government objectives
- ensuring that the department's management practices for service, information, data and IT:
  - align with the direction set by the Office of the Chief Information Officer of TBS
  - follow legislative requirements for protecting privacy
- supporting the department and senior leaders in open and digital transformation
- ensuring that IT, information and data activities align with government-wide and departmental service priorities and strategies

In addition to "consulting with the CIO of Canada before appointing, deploying, or otherwise replacing the departmental CIO" (subsection 4.5.2.3 of the *Policy on Service and Digital*), deputy heads may consider the following when designating a departmental CIO:

- leadership competencies

- knowledge of enterprise information and IT solutions and transformation in a dynamic and complex environment
- knowledge of service, IT, information and data technology functions
- knowledge of domestic or international partnerships to achieve departmental and government-wide outcomes
- understanding of IT, information, privacy protection and data governance
- understanding of work, workplace and workforce issues, trends, solutions and practices
- understanding of emerging government-wide direction on digital services and their impact on the department
- understanding of how the management of technology, information and data can help support and enable departmental and government-wide services

In discussions related to the appointment, deployment or replacement of a departmental CIO, deputy heads must ensure that "for the purposes of the Treasury Board Executive Group (EX) Qualifications Standard, the departmental CIO possesses an acceptable combination of education, training and experience" (subsection 4.5.2.4 of the *Policy on Service and Digital*). This requirement is mirrored at the government-wide level where the CIO of Canada is responsible for "providing enterprise-wide leadership on knowledge standards for the information and IT community, including determining the acceptable combination of education, training and experience required for the Treasury Board Executive Group (EX) Qualification Standard" (subsection 4.5.1.2 of the *Policy on Service and Digital*).

Considerations for designating an official responsible for leading the departmental cyber security management function

The role of the designated official for cyber security (DOCS) is to provide department-wide strategic leadership, coordination and oversight on cyber security, in collaboration with the departmental CIO and chief security officer (CSO), as appropriate. The DOCS is responsible for:

- ensuring that cyber security requirements and appropriate measures are applied in a risk-based, life-cycle approach to protect IT services, in line with the *Directive on Security Management*, Appendix B: Mandatory Procedures for information Technology Security Control
- clearly identifying and establishing roles and responsibilities for reporting cyber security events and incidents in accordance with section 5 of the Government of Canada Cyber Security Event Management Plan and subsection 4.1.6 of the *Directive on Security Management*, and undertaking immediate action if there is a privacy breach and implementing associated mitigation measures

It is recommended that deputy heads consider the following when designating a DOCS:

- knowledge and awareness of domestic and international cyber security related trends, risks and their impacts

- knowledge of Government of Canada and departmental policy instruments relating to cyber security, the department's business context and threat environment, and the department's overall cyber security posture
- ability to enable strategic discussions regarding cyber security–risks, and to support integrated and informed risk management decisions at a senior official level

Taken together, these considerations are important because they provide deputy heads with an integrated view of government cyber security practices, risks and concerns.

The responsibilities of the DOCS in a small department or agency would be the same as that for a larger department. Regardless of a department's size, capacity should be considered when designating the DOCS to ensure that the designated individual can effectively fulfill their responsibilities. For example, the deputy head could designate the CSO as the DOCS if doing so appears to be a good fit. In larger departments and agencies, it may be preferred to have another senior official designated as the DOCS. Specific responsibilities of the DOCS and the CSO in relation to cyber security would be defined in the integrated departmental governance.

1.3 Integrated planning and reporting

1.3.1 Description and associated requirements

The three policy requirements under this theme focus on the integration of planning and reporting of service, information, data, IT and cyber security.

Requirement for TBS under the policy
The **CIO of Canada** is responsible for: 4.1.2.7 Approving an annual, forward-looking three-year enterprise-wide plan that establishes the strategic direction for the integrated management of service, information, data, IT, and cyber security and ensuring the plan includes a progress report on how it was implemented in the previous year.

This policy requirement mandates the CIO of Canada to produce an integrated government-wide plan and ensure that it:

- provides overarching enterprise-wide direction for managing service, information, data, IT and cyber security
- is issued annually and covers the next three years
- includes a progress report that provides a measured assessment of how the plan for the previous year was implemented

Requirement for departments under the policy
Deputy heads are responsible for: 4.1.3.7 Approving an annual forward-looking three-year departmental plan for the integrated management of service, information, data, IT, and cyber security, which aligns with the CIO of Canada's enterprise-wide integrated plan, is informed by subject-specific plans or strategies as appropriate, and includes a progress report on how it was implemented in the previous year.

This policy requirement mandates deputy heads of departments to produce an integrated departmental plan. Deputy heads must ensure that the plan:

- provides overarching direction for the integrated management of service, information, data, IT and cyber security within their organization
- is informed by subject-specific plans as appropriate
- is issued annually and covers the next three years
- is aligned with the CIO of Canada's enterprise-wide integrated plan

- includes a progress report that will provide a measured assessment of how the previous plan was implemented

Requirement for departments under the directive
Departmental CIOs are responsible for: 4.1.1.7 Producing the departmental IT expenditure report and on-going Application Portfolio Management update reports.

This requirement mandates departmental CIOs to produce:

- a departmental IT expenditure report
- ongoing Application Portfolio Management program

1.3.2 Why is this important?

There are several benefits to integrating planning and reporting across service, information, data, IT and cyber security. An integrated approach:

- supports effective planning and better decision-making by ensuring collaboration and due consideration of interrelated management areas
- focuses on service and comprehensive digital enablement, with particular attention to proactive consideration in designing and developing government services and other activities
- provides for a more holistic approach to planning and reporting, which allows key interdependencies to be identified, including identifying systems that have limited business value and opportunities to reallocate investments in areas that support service delivery
- ensuring that client-centric services to Canadians is supported by establishing, measuring and assessing targets, integrated planning and reporting

1.3.3 Considerations in implementing the requirements

Departments remain expected to follow current instructions and produce individual plans and reports. No changes are required for departments' plans and reports in 2020–21. TBS, in collaboration with departments, will be developing additional and updated guidance and tools to set out expectations for integrated planning and reporting.

Integrated departmental plan

A departmental integrated plan is to outline how service, information, data, IT and cyber security will be managed within the department. The plan must align to the CIO of Canada's government-wide plan that provides the strategic direction and priorities for the Government of Canada with respect to the same areas of management service. By aligning their own plans with that of the CIO of Canada, departments will support the government's direction.

Departments' progress in achieving the strategic goals outlined in the CIO of Canada's enterprise plan will be tracked, evaluated and reported on annually at the enterprise level. Departments, through their integrated plans, will detail how the enterprise approach will be implemented within their organization. Departments' integrated plans will be leveraged to support enterprise priorities, such as:

- improving services provided to Canadians
- providing sound information and data stewardship
- ensuring secure and sustainable IT infrastructure and systems

IT Expenditure Report

In 2011, the Comptroller General of Canada and the CIO of Canada jointly issued a request to some departments for information on departmental IT expenses. TBS asked those organizations to:

- use a "high-level" expenditure model to create a baseline for Government of Canada IT expenses, starting with data from 2009–10
- maintain this data for each fiscal year on an ongoing basis

Collection of such information has continued as the IT Expenditure Report, which collects departmental spending on IT by fiscal year and helps inform decision-making.

Context and guidance for departments on developing an IT Expenditure Report is available on the IT Expenditure GCwiki page (available only on the Government of Canada network).

Application Portfolio Management Program

The TBS Application Portfolio Management Program aims to:

- improve the maturity of application portfolio management practices across government to provide a holistic view of the Government of Canada applications landscape, related risks and investments
- support government-wide strategies on the renewal and evergreening of aging applications that are economical and that ensure continued services to Canadians
- Direct investments towards government priorities, by implementing as part of investment planning, multi-year planning for applications that is interlocked with corporate risk
- populate Shared Service Canada inventories to help provide responsive and tailored client support

Context and guidance for departments on developing an Application Portfolio Management Report is available on the GCwiki Application Portfolio Management (APM) page (available only on the Government of Canada network).

Other considerations in implementation: broader alignment

In addition to ensuring integrated planning to manage service, information, data, IT and cyber security, other Treasury Board policies require deputy heads to ensure alignment with other areas of management, such as financial management and investment planning, including project management, procurement, materiel management and real property. For example, it is recommended that a department's capacity for the following be considered in setting strategic direction, prioritization and impact:

- financial management
- investment planning
- procurement and project management
- capacity of service providers

1.4 Enterprise architecture governance

1.4.1 Description and associated requirements

Enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. It takes into consideration and seeks to align the various domains in an organization, such as:

- business
- information and data
- applications
- technology
- security privacy protection

EA leads an organization toward an integrated and unified enterprise system that is better positioned to achieve strategic outcomes and create business value than if the organization operated in silos.

Governance for EA at the enterprise level is conducted through the Government of Canada Enterprise Architecture Review Board (GC EARB), which oversees the implementation of the EA direction for the Government of Canada. The objective of enterprise-level EA governance is to ensure that departmental vision and standards are aligned with Government of Canada EA requirements.

Requirements for TBS under the policy
The **CIO of Canada** is responsible for: 4.1.2.3 Prescribing expectations with regard to enterprise architecture. 4.1.2.4 Establishing and chairing an enterprise architecture review board that is mandated to define current and target architecture standards for the Government of Canada and review departmental proposals for alignment.

The *Directive on Service and Digital* outlines when departments must appear before the GC EARB and how to establish their own departmental architecture review board (DARB).

Requirements for departments under the directive

The **departmental CIO** is responsible for:

4.1.1.1 Chairing a departmental architecture review board that is mandated to review and approve the architecture of all departmental digital initiatives and ensure their alignment with enterprise architectures.

4.1.1.2 Submitting to the Government of Canada enterprise architecture review board proposals concerned with the design, development, installation and implementation of digital initiatives:

4.1.1.2.1 Where the department is willing to invest a minimum of the following amounts to address the problem or take advantage of the opportunity:

4.1.1.2.1.1 $2.5 million dollars for departments that do not have an approved Organizational Project Management Capacity Class or that have an approved Organizational Project Management Capacity Class of 1 according to the *Directive on the Management of Projects* and Programmes;

4.1.1.2.1.2 $5 million dollars for departments that have an approved Organizational Project Management Capacity Class of 2;

4.1.1.2.1.3 $10 million dollars for departments that have an approved Organizational Project Management Capacity Class of 3;

4.1.1.2.1.4 $15 million dollars for the Department of National Defence;

4.1.1.2.1.5 $25 million dollars for departments that have an approved Organizational Project Management Capacity Class of 4;

4.1.1.2.2 That involve emerging technologies;

4.1.1.2.3 That require an exception under this directive or other directives under the policy;

4.1.1.2.4 That are categorized at the protected B level or below using a deployment model other than public cloud for application hosting (including infrastructure), application deployment, or application development; or

4.1.1.2.5 As directed by the CIO of Canada.

4.1.1.3 Ensuring that proposals submitted to the Government of Canada enterprise architecture review board have first been assessed by the departmental architecture review board where one has been established.

4.1.1.4 Ensuring that proposals to the Government of Canada enterprise architecture review board are submitted after review of concept cases for digital projects according to the "Mandatory Procedures for Concept Cases for Digital Projects" and before the development of a Treasury Board submission or departmental business case.

4.1.1.5 Ensuring that departmental initiatives submitted to the Government of Canada enterprise architecture review board are assessed against and meet the requirements of Appendix A:

Mandatory Procedures for Enterprise Architecture Assessment and Appendix B: Mandatory Procedures for Application Programming Interfaces.

1.4.2 Why is this important?

IT spending has not always been coordinated across government, leading to duplicated effort and resources, with no clear goals for improving services and operations. This approach revealed the need for better coordination, within and between departments, in order to:

- decrease duplicative spending
- increase interoperability
- provide more cohesive government services

EA supports a coordinated approach by providing an integrated view of IT spending and priorities that will help the government optimize its IT investments. EA governance at the enterprise level ensures that all departmental digital initiatives that meet criteria of subsection 4.1.1.2 of the *Directive on Service and Digital*):

- are reviewed at the GC EARB
- align with Government of Canada EA standards (see the directive's Appendix A: Mandatory Procedures for Enterprise Architecture Assessment and Appendix B: Mandatory Procedures for Application Programming Interfaces)

In addition, cost efficiencies can be achieved through sharing lessons learned, procurement vehicles and investments.

1.4.3 Considerations in implementing the requirements

To ensure clear direction and to guide departments on aligning with government-wide direction and strategies for EA, the following mandatory procedures are included in the *Directive on Service and Digital*:

- Appendix A: Mandatory Procedures for Enterprise Architecture Assessment
- Appendix B: Mandatory Procedures for Application Programming Interfaces

Appendix A of this guideline provides an assessment framework to review digital initiatives to be used by DARBs and the GC EARB. Appendix B of this guideline provides details on subsection A.2.3.10.3 of the Mandatory Procedures for Enterprise Architecture Assessment, which relates to the use of application programming interfaces to:

- allow communication between IT services
- enable interoperability

Do you need to make a proposal to the GC EARB? To find out, follow these steps

1. Conduct a self-assessment against the criteria outlined in subsection 4.1.1.2 of the *Directive on Service and Digital*.
2. If one or more of the criteria apply, the proposal is to be submitted to the GC EARB.
3. Ensure that the proposal follows the review of concept cases for digital projects, before the development of a Treasury Board submission or a Departmental Business Case. Refer to the Mandatory Procedures for Concept Cases for Digital Projects.
4. Ensure that the proposal meets the requirements of Mandatory Procedures for Enterprise Architecture Assessment and Mandatory Procedures for Application Programming Interfaces.
5. Bring the proposal to your department's DARB for assessment, before submitting it to the GC EARB.
6. Once the DARB has assessed the proposal, the presenter can complete the GC EARB Presenter Template and submit the proposal by email to:

   Enterprise Architecture Team
   Office of the Chief Information Officer
   Treasury Board of Canada Secretariat
7. Once received, the proposal is reviewed against the requirements of the Mandatory Procedures for Enterprise Architecture Assessment.
8. Once reviewed, the Office of the Chief Information Officer EA team:
   - provides feedback to the presenter on the proposal in advance of the presentation at the GC EARB
   - briefs the GC EARB co-chairs
9. The GC EARB co-chairs review the final proposal. If there are no issues, the GC EARB secretariat will invite the departmental contacts to present their proposal at a regularly scheduled meeting of the GC EARB.

For more information, visit the GCwiki Enterprise Architecture Review Board web page (available only on the Government of Canada network), which includes information such as the GC EARB's agendas, past sessions, and other useful links and resources.

Additional resources include:

- Enterprise Architecture Community of Practice: This group discusses a range of topics related to EA in the Government of Canada. The group has subgroups for each of the EA layers, including :
  - business architecture
  - information architecture
  - application architecture
  - technology architecture
  - security and privacy architecture

  The group's resources include:

  - target architectures developed by departments
  - a draft Government of Canada Service and Digital Target architecture
- GC Enterprise Architecture wiki (available only on the Government of Canada network). This page provides details on the various layers of EA.

1.5 Innovation and experimentation

1.5.1 Description and associated requirements

Coming up with innovative ideas can be relatively easy, fast and cheap, but executing such ideas is where matters become more complex. This is especially true in a context where enterprise-wide standardization is prioritized to achieve increased interoperability and other government-wide outcomes, such as improved government services and operations.

In TBS's Experimentation Direction for Deputy Heads: December 2016, experimentation is defined as "testing new approaches to learn what works and what does not work using a rigorous method." This direction identifies possible features that an experimentation project could have, as well as potential innovative approaches, including tools and methods. In this direction, innovation is regarded as finding new ways to address problems. Experimentation is vital to innovation because turning an idea or concept into a meaningful reality must be tested before release.

At the departmental level, the process of providing the appropriate level of support to take an idea, refine it, experiment with it and turn it into a real solution is what this requirement is about. At the government-wide level, the CIO of Canada plays a role in facilitating this process by providing tools and guidance in support of innovation and experimentation, including establishing guidance on open-source and open-standard applications, and agile application development.

Requirements for TBS under the policy	
The **CIO of Canada** is responsible for:	
4.1.2.6	Facilitating innovation and experimentation in service design and delivery, information, data, IT and cyber security.
4.4.1.6	Establishing guidance to support innovative practices and technologies, including open-source and open-standard applications, and agile application development.

Requirement for departments under the policy	
The **deputy head** is responsible for:	
4.1.3.8	Providing support for innovation and experimentation in service, information, data, IT and cyber security.

1.5.2 Why is this important?

Digital technologies are changing constantly. Often, the operational necessities of managing an organization present little opportunity to research and implement new technologies. Therefore, deputy heads need to support specific activities to review, assess and potentially adopt new methods to better support departmental priorities and improvements to services and operations in the long run.

The benefits of adopting innovation and experimentation include the following:

- finding new ways to address persistent problems that traditional approaches have failed to solve
- generating evidence to learn what works and it inform decision-making
- delivering services to the public using tools that are modern and effective to meet client expectations
- empowering employees to bring forward new ideas
- allowing to keep pace with rapidly evolving technological changes and avoid the use of outdated tools

1.5.3 Considerations in implementing the requirements

In December 2016, the Experimentation Direction for Deputy Heads was issued by TBS to reinforce the government's commitment to devote a fixed percentage of program funds to experimenting with new approaches and measuring impact. Although program funding is one way of providing "support" for innovation and experimentation, there are other methods that deputy heads can use, based on their department's size, mandate and other factors. For example, deputy heads can support their organization by putting in place:

- internal activities ("Dragons' Den" events, hackathons)
- supporting structures (innovation hubs)
- employee-focused activities (awareness, time allotments, training)

In providing support for innovation and experimentation, departments could consider implementing the following practices:

- developing proof of concepts and pilot projects as a way to learn quickly before launching on a full scale
- creating an environment that supports cross-departmental collaborations
- creating a dedicated research and development team with operational resources frequently rotating in and out
- developing an environment that allows for the isolated execution of software or programs for independent evaluation, monitoring or testing, without affecting the application, system or platform on which they run (sandbox environments) to enable the safe incubation of disruptive projects
- using fictional data (data created from scratch that do not include personal information and that do not represent or identify Canadian citizens) in innovation and experimentation solutions to eliminate risks of information exposure or privacy breaches
- using modern and agile practices in software development to reduce implementation timelines

- leveraging open-source and open-standard applications to avoid duplicating efforts and allow for community-based improvements
- partnering with external stakeholders such as universities to establish events such as hackathons (using open data) to help innovate

Pilots and proof of concepts can be submitted to the GC EARB for review and assessment. GC EARB provides recommendations on new processes and technology when conducting assessments. Subsection 1.4 of this guideline has more information on GC EARB assessments.

In order to share and promote innovation and experimentation broadly within the Government of Canada, and to showcase successful practices and learn from challenges, departments should incorporate activities for their innovation and experimentation projects into their departmental planning processes.

Innovation and experimentation activities, as for any other activities undertaken in departments, must comply with all related laws and Treasury Board policies, including requirements for privacy protection, security and accessibility.

In addition, if you are collecting, using or disclosing personal information, the use of fictional data is recommended for innovation or experimentation. Contact your institution's Access to Information and Privacy (ATIP) office to discuss the requirement for a Privacy Impact Assessment, as required by the *Directive on Privacy Impact Assessment*. Subsection 3.6 of this guideline has more information on specific considerations related to privacy and protection of personal information.

It is also important to prioritize security at the outset of innovation and experimentation activities. For more information on security considerations, see subsection 4.1 of this guideline. In the context of cloud, additional security controls may need to be considered in order to satisfy departmental requirements. For more information on security considerations related to cloud services, see subsection 4.3 of this guideline.

There is also an opportunity to experiment with new ways of enabling accessibility across the government, whether it is related to accessible information and communication technology or creating accessible documents from the outset. See subsection 3.5 of this guideline for more information on accessibility requirements.

In line with the requirement of the CIO of Canada to support innovative practices and technologies, including open-source and open-standard applications and agile application development, further guidance on Open Source Software and an Open First Whitepaper are available for departmental use. Departments that are interested in additional research and guidance for open source in government can join the TBS-led FLOSSING community of practice.

2. Client-centric service design and delivery

Every day, the Government of Canada delivers a broad range of services to Canadians. Excellence in designing and providing services promotes confidence in government and contributes to the efficient and effective achievement of public policy goals and better services for Canadians.

In an effort to continually improve its services, the Government of Canada has adopted a vision where:

- client needs and feedback are at the centre of service design and delivery
- services are simple, seamless, transparent, digitally enabled, and available anytime and anywhere

Among the expected outcomes of the *Policy on Service and Digital* is the development of departmental capacity to facilitate client-centric service design and delivery.

This section outlines the following key components:

- implementing client-centric service design, delivery and improvement
- maximizing the availability of end-to-end online services to complement all service delivery channels
- establishing a departmental service inventory that is updated annually
- developing service standards, related targets and performance information
- undertaking service reviews

Appendix B of this guideline contains information on service definition, identification and types of services.

This section of the guideline replaces the guidance provided in the *Guideline on Service Management*, which was developed in support of the *Policy on Service*.

2.1 Client-centric services

2.1.1 Description and associated requirements

Client-centric services focus on addressing client or user expectations, needs, challenges and feedback. Such services create a positive experience for the client or user and consider several factors, such as:

- access
- inclusion
- accessibility
- security
- privacy
- simplicity
- choice of official language

A service-oriented government puts clients and their needs as its primary focus. A central component of this approach is understanding the needs of clients and building services around clients rather than concerns about organizations or silos.

Requirement for departments under the policy
Deputy heads are responsible for: 4.2.1.1 Ensuring the development and delivery of client-centric service by design, including access, inclusion, accessibility, security, privacy, simplicity, and choice of official language.

2.1.2 Why is this important?

The government has an opportunity to better understand its citizens and their needs, and tailor services accordingly, when it considers client needs and feedback throughout the design and delivery of a service. A successful digital government continually improves how it designs and delivers services to improve the lives of its citizens, while maximizing the opportunities presented by information and technology to do so.

2.1.3 Considerations in implementing the requirement

When designing services, departments should consider several factors related to client-centric service, including the following:

Access

Today, clients increasing expect to access the services they need, when and where they want, whether it be online, by phone or in person. This requires an omni-channel approach for all services in order to:

- offer Canadians an integrated customer experience
- enable the modernization of Government of Canada services

Departments can leverage the use of technology and automation across all service delivery channels, including in-person services and call centres, to increase their efficiency and improve the client experience.

Examples

OneGC is the enterprise approach to enable seamless service delivery through interoperable systems, data-sharing and greater integration between services. OneGC is the umbrella under which common technology solutions and experimental service initiatives are pursued, in support of the digital government vision, where services are optimized for digital and are available anytime, anywhere and from any device.

An additional example is the use of digital identity to identify and authenticate users and provide them with more seamless and secure enrolment and access to online services. See subsection 4.7 of this guideline for more information.

Inclusion

As the Government of Canada builds its capacity to offer more efficient client-centric services, there is an opportunity to bring about a culture shift to foster greater social inclusion. Such inclusion improves the participation of groups in society, particularly for people who are disadvantaged, through enhancing opportunities, access to resources, greater participation and respect for rights. Further information is available in see the Inclusive Design Guide prepared by the Inclusive Design Institute (IDI).

Accessibility

When designing services, departments are to ensure that they are barrier-free for Canadians by making them inclusive, accessible by default and usable by the broadest range of citizens and employees without special adaptation.[2] See subsection 3.5 of this guideline for more information on specific considerations related to accessibility.

ESDC's Accessible Client Service Centre of Expertise has been working with partners to develop tools to support ESDC become more accessible. These tools can be used more broadly to support the government-wide effort.

Security

When designing services, departments are to:

- consider today's dynamic operating environment, which is increasingly global and features:
    - a highly mobile workforce
    - shared IT
    - shared service delivery

[2] Does not preclude adaptation for specialized needs in specific circumstances.

- strengthen government security management

Cyber security is an important and ever-evolving aspect of any government technology strategy to ensure continuity of service and safeguard citizens' private information. Consolidated programs, online end-to-end services and "tell us once" approaches increase the importance of cyber security, as information that is more consolidated or connected can intensify the impacts of security breaches, including privacy breaches. See subsection 4.6 of this guideline for more information on specific considerations related to cyber security.

Privacy

The requirements of the *Privacy Act*, the *Privacy Regulations* and associated policies for the effective protection and management of personal information must be integrated throughout the design and delivery of services and systems. These requirements include the following:

- limiting the collection of personal information to only what is directly related to delivering a service
- ensuring that clients are notified in advance about why their personal information is being collected and how it will be used
- ensuring that personal information is used only in ways that have been communicated to clients
- sharing personal information only as permitted by law
- keeping information only for as long as required

See subsection 3.6 of this guideline for more information on specific considerations related to privacy.

Simplicity

Whether services are provided in person, by telephone or online, it is important that they be simple for the client or user. Various factors contribute to this experience, including using:

- clear language
- appropriate formats
- simplified interaction processes
- user-friendly guidance (text boxes, YouTube videos, pamphlets) when necessary

Official languages

When designing and delivering services, departments must:

- support activities that benefit members of both official language communities
- respect the obligations of the Government of Canada as set out in Part VII of the *Official Languages Act*, including ensuring that services are made available in both official languages

Departments should also comply with the *Policy on Official Languages*.

2.2 Client feedback and satisfaction

2.2.1 Description and associated requirements

Client feedback is information directly from recipients of services about their satisfaction or dissatisfaction with a service or product. It is a key part of service improvement and can take several forms, including the following:

- in-service client feedback
- client satisfaction surveys
- user experience design and testing
- consultations

Requirement for departments under the directive
The **designated official for service**, in collaboration with other officials as necessary, is responsible for: 4.2.1.1 Ensuring that client feedback, including in-service client feedback, client satisfaction surveys and user experience testing, is collected and used to improve services according to TBS direction and guidance.

2.2.2 Why is this important?

Client feedback is important to delivering services that meet the needs of clients and to continual improvement. They serve several key purposes, including the following:

- identifying areas of service design and delivery that require improvement
- contributing to the overall evaluation of client satisfaction with the organization's services
- providing an opportunity to establish trusting relationships with clients and the organization by assisting clients in overcoming service-related challenges
- increasing operational efficiency and effectiveness by identifying and addressing systemic service delivery issues

2.2.3 Considerations in implementing the requirement

Mechanisms to provide feedback can include various methods or tools, formal or informal, to:

- collect feedback from clients
- resolve service issues not related to decisions or appeals

Examples of feedback channels are an ombudsman, a generic departmental email or social media account, and questionnaires during service delivery.

Client feedback mechanisms allow departments to receive and manage input from clients and involve recording, processing, responding to and reporting on the input received. These mechanisms supplement user experience design, which supports the development of products that provide meaningful and relevant experiences to users.

When services are delivered by a group of partners (such as Canadian or international organizations, or other levels of government such as provinces, territories and municipalities), departments are to work with them to develop and process client feedback.

Feedback mechanisms are used to manage a broad range of client experience information and usually employ several methods across all service delivery channels (in person, telephone and online), both prompted and unprompted. For example:

- feedback mechanisms that involve prompting users for input include offers to participate in an exit survey
- an unprompted method could include a "contact us" section that includes a web link, generic email and/or telephone number to contact the department

When departments seek client feedback, they should consider the Government of Canada's public engagement principles.

Information received through the feedback mechanism can be classified into two broad categories:

1. general feedback used to improve services, including future service improvement work plans
2. more specific feedback or complaints on service delivery issues that are likely to require interaction or follow-up with a client, with varying degrees of urgency

Addressing service issues

A service issue refers to a challenge that a client is experiencing at any point in the process of receiving a service. It does not relate to recourse related to a decision or a formal appeal process.

Although most service issues are minor, they typically require immediate attention in order to be resolved in a timely manner, which is important to providing an overall positive service experience for the client. How quickly these issues are resolved will depend on their complexity and the operational circumstances of the organization. Examples of service issues that could be addressed by the mechanism include the following:

- seeking clarification on what information is required to submit a complete application
- overcoming difficulty with a web page, registering or authenticating a departmental account, or submitting an application
- enquiring about the status of an application

Service issues are routinely raised with client service officers during normal client interactions and can usually be resolved quickly, to the clients' satisfaction or understanding during the initial contact. To the extent possible, these interactions should be recorded to inform service management improvement.

Determining whether an issue identified by a client is eligible for consideration under a particular mechanism can help avoid wasting resources on a misunderstanding, a wrongly directed concern, or a frivolous matter. For example, if a client's application for a permit is denied, their perceptions of the service delivery and the decision taken may be negative, when in fact the delivery of the service met or exceeded established service standards. In this case, the outcome of the transaction is influencing the client's satisfaction with the service.

Depending on the type of information and the circumstances involved, a single method may be used to collect feedback and resolve service issues. In certain departmental situations that involve a large volume of services and transactions, a specific office dedicated to client feedback and service resolution, such as an office of client satisfaction, could be considered.

Examples of client feedback methods include the following:

- generic links for comments, compliments and complaints on the organization's web presence
- a web pop-up during or after service delivery interactions
- a service agent recording verbal input during an in-person or telephone visit
- an electronic kiosk at in-person centres where feedback can be submitted
- a service exit survey
- an external stakeholders reference group
- public opinion research (for example, client satisfaction surveys)

Examples of methods to resolve client-service issues include the following:

- an online live chat function
- online co-browsing with a service agent
- a telephone or in-person conversation with a service agent
- a departmental response to the client via email
- reference to a repository of frequently asked questions

Characteristics of effective client feedback

1. **Easily accessible:** Feedback should be easily identifiable by clients, and its availability should be actively promoted across all service channels. Clients who wish to provide feedback or require assistance to resolve a service issue need to know how to provide it and to whom, and this information should be readily available and clear. Consider the following:
    - Does the department proactively provide information to clients about how to provide feedback through all service delivery channels? How is this information disseminated?
    - Are there suitable arrangements to allow people with disabilities to provide feedback or raise issues?
2. **Broad in scope:** Feedback mechanisms designed to obtain a representative response from all client groups will provide more balanced feedback and allow for better overall service management. Such mechanisms may involve multiple feedback methods targeted at different clients to maximize the diversity of views and effectiveness of service improvement responses. Front-line employees often experience direct indications of satisfaction through client reactions on a daily basis, and this data should be collected as well. Beware, however, of response biases, which can occur in situations of

voluntary response, where those who care enough to respond may have either extremely negative or positive opinions, and may not necessarily be a statistically representative sample of the actual population. Implementing change to respond to client feedback also requires a strategic, whole-system approach, including considering the impact of improving results in one area of performance or another. For example, focusing on reducing transaction time to improve client satisfaction may, if not carefully considered, negatively impact service quality, in turn resulting in lower client satisfaction.

3. **Simple for clients:** Feedback and issue-resolution mechanisms, regardless of the service delivery channel (for example, online, in person, or telephone) should be simple for clients to understand and use. Consider the following:
   - Is guidance on using the feedback mechanisms available for clients?
   - Is the format and language used to collect feedback easily understandable by the service's target clients?
4. **Staff engagement and training:** Internally, procedures designed to guide employees in collecting and managing feedback should be applied consistently across the department. Approaches to resolving issues, however, may sometimes vary according to the type and nature of the issue. Consider the following:
   - Are written procedures or guidance on feedback and mechanisms to resolve issues available to employees?
   - Does the department review guidance and feedback procedures regularly?
   - Has the department designated staff to help address client feedback issues?
   - Do the procedures set out clear responsibilities for designated staff?

   All employees who deal with clients regularly should receive training in how to handle various issues. Such training could include instruction in negotiation, alternative dispute resolution, and dealing with difficult people. Consider the following:
   - Do procedures allow employees to resolve issues on the spot if possible, and to provide immediate resolution, where appropriate?
   - If employees cannot deal appropriately with an issue immediately, do the procedures identify the key steps for conducting a full review and for providing a full final reply?
   - Are there standardized procedures for dealing with various types of issues and for each step in responding to clients, such as acknowledgment, interim reply and final reply?
   - Does the department's client relations management system allow employees to access information about an issue quickly?

5. **Privacy risks mitigated:** Feedback processes and mechanisms must respect privacy requirements, in accordance with the *Privacy Act*, the *Privacy Regulations* and related policies. Staff involved in the feedback process must be aware of their privacy obligations when collecting and using feedback.

Unauthorized collection, use, retention or disclosure (including sharing) of personal information constitutes a privacy breach. For example, collecting feedback through open text fields can inadvertently over-collect personal information, leading to privacy breaches. When reporting on feedback metrics, the data must be aggregated so that individuals cannot be re-identified. In addition, if third-party researchers are engaged, staff should ensure that contracts include privacy protections. For assistance, contact your institution's ATIP office.

6. **Responsiveness:** Capturing and responding to client feedback in a comprehensive and timely manner is important in addressing negative experiences. For complex cases that require more time for follow-up, clients should be kept informed of the progress on addressing the issues they have raised throughout the feedback and issue-resolution process.
7. **Monitoring and reporting:** Most leading organizations establish performance metrics related to client feedback and issue resolution and collect data to monitor their own performance. The frequency of data collection should correspond to the nature of the service and the frequency and nature of client interactions. A positive outcome or improvement in service resulting from client feedback or issue resolution demonstrates responsiveness and may improve the public's confidence in government programs and services in the long term. It is therefore important to publicly report on issues analysis and to show where such analysis has led to improvements. Providing clients with an opportunity to view a summary of survey results or actions undertaken in response to comments, complaints and suggestions will provide transparency, demonstrate that their feedback is valuable, and encourage their continued participation. Consider the following:
    - Has the department made service improvements after assessing issues raised by clients?
    - Has the department released open data and information on feedback received and improvements made?

8. **A corporate-wide approach:** The adoption of a corporate-wide approach allows for a more consistent client experience and provides greater insight into identifying and addressing service issues. Public opinion research can shed important insights into overall client satisfaction with services.
9. **Third-party research on client satisfaction:** Third-party research on client satisfaction can provide valuable insight into how to improve the client experience. When assessing client satisfaction, consider the following key indicators:
    - timeliness
    - courtesy
    - ease of access
    - ease of completing the transaction

2.3 Online services

2.3.1 Description and associated requirements

The *Policy on Service and Digital* defines online services (sometimes referred to as e-services) as services available on the Internet from beginning to end, without the client having to move offline to complete a step in the process. These services include the ability to receive a service online from the application stage, to the receipt of the final output and the provision of feedback. The final output may not be delivered online in all cases, as it may be a material document, such as a passport, a certificate or other item. However, departments are encouraged to consider the possibility of providing the final output online as well.

In instances of third-party delivery, departments have to incorporate online requirements into their contracts or agreements, as compliance with the *Policy on Service and Digital* remains necessary in those situations.

Requirement for departments under the policy
Deputy heads are responsible for: 4.2.1.2 Maximizing the online end-to-end availability of services and their ease of use to complement all service delivery channels.

2.3.2 Why is this important?

Jurisdictions within Canada and around the world are increasingly focusing their efforts on delivering a better online service experience that clients want to use. Canadians and businesses have been clear that they expect online government services that:

- are accessible, fast and personalized
- respect privacy
- are secure

Online services are convenient for clients and are significantly more cost-effective than services delivered through in-person or telephone channels.

It is important to pursue holistic and integrated online delivery of services. Requiring clients to download and print an online PDF file, complete it, and send it to a Government of Canada office by fax or email is considered to be "out of band" and not an online service. Moreover, this is not what clients expect as an online service and is inefficient.

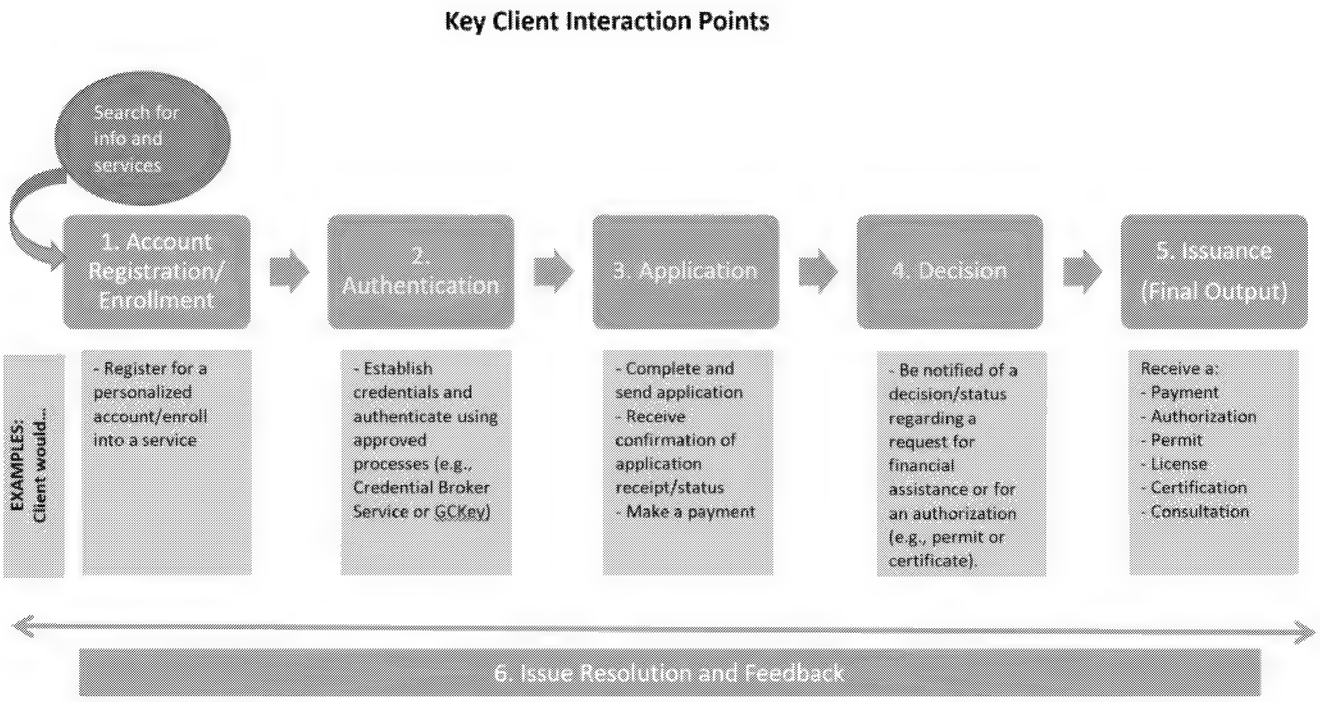
2.3.3 Considerations in implementing the requirement

The availability of an online service usually applies to all the interaction points between the service provider and the client. Typically, key interactions include (may not be limited to) the following six points:

1. **Account registration and enrolment:** This step is where the client registers for a personalized account in order to request the service (for example, a veteran registering for a MyVAC account).
2. **Authentication:** This step is where the client provides information and where their credentials are authenticated (for example, GCKey).
3. **Application:** This step is where the client completes and submits their request, receives confirmation that the request has been registered, and provides payment if required (for example, completing an application for a social insurance number).
4. **Decision:** This step where the client is notified of the outcome of the request (for example, confirmation on whether a client qualifies for Employment Insurance).
5. **Issuance (final output):** This step is where the client receives the service (for example, payment, permit, licence or information).
6. **Issue resolution and feedback:** This step is where issues encountered during the delivery cycle are captured, reviewed, addressed and recorded, and where feedback on the service experience is provided (for example, online chat with a service agent or client service feedback).

Figure 1 illustrates the key client interaction points described above.

Figure 1: Key client interaction points


Key Client Interaction Points
Search for info and services
1. Account Registration/ Enrollment
2. Authentication
3. Application
4. Decision
5. Issuance (Final Output)
EXAMPLES: Client would...
- Register for a personalized account/enroll into a service
- Establish credentials and authenticate using approved processes (e.g., Credential Broker Service or GCKey)
- Complete and send application
- Receive confirmation of application receipt/status
- Make a payment
- Be notified of a decision/status regarding a request for financial assistance or for an authorization (e.g., permit or certificate).
Receive a:
- Payment
- Authorization
- Permit
- License
- Certification
- Consultation
6. Issue Resolution and Feedback

Considerations

1. When establishing plans to increase the proportion of online services, consider the following:
    - start with the department's most-sought services and broaden the scope over time based on key factors such as volume of service, cost or benefit, and risk
    - collaborate with key partners, such as the department's CIO, its web senior departmental official, and other Government of Canada institutions that offer similar services
2. Ensure that privacy- and security-related considerations are addressed at the design stage. For more information, refer to subsection 4.1 of this guideline.
3. The *Standard on Privacy and Web Analytics* provides detailed instructions to institutions for collecting, using, retaining and disclosing personal information for web analytics. The standard requires that users are notified through a privacy notice statement prior to collecting personal information. Contact your ATIP office early in the design process. It will help you assess:
    - whether the new system will collect and use personal information
    - whether a Privacy Impact Assessment needs to be completed (the assessment will address how the service will respect the requirements of the *Privacy Act*).
4. Leverage trusted digital identity to identify and authenticate users, and to provide more seamless and secure enrolment and access to online services. For more information on digital identity considerations, refer to subsection 4.7 of this guideline.

5. The *Standard on Web Usability* ensures that Government of Canada websites and web applications respect usability principles and approaches. New websites and web applications must meet the requirements of Section 6 of the standard when they are published. In addition, *Technical Specifications for the Web and Mobile Presence* describes how to optimize:
    - websites and web applications for mobile devices
    - layout and design specifications for websites, web applications and device-based mobile applications
6. The *Content and Information Architecture Specification*, in conjunction with the *Canada.ca Web Content Style Guide* provide content-related guidance for departments as they prepare themselves for migration. The specification provides:
    - a blueprint for how content on Canada.ca is to be organized
    - templates and guidelines for departments to rework, develop and harmonize content as they prepare to migrate their content to the Managed Web Services platform and decommission their URLS
    - information architecture requirements, which are key to effectively align the implementation of the Managed Web Services platform
7. When designing online services, consider the use of application program interfaces (APIs) as a means to facilitate this work. Refer to subsection 3.3 of this guideline for further details.

User engagement

User engagement promotes awareness among clients of the availability of online services and the benefits of accessing and using them, with the ultimate goal of increasing uptake. Following are some key points to consider when engaging users on online services:

- Incorporate user engagement into departmental service improvement plans. Departments can articulate their engagement approaches or priorities within service management plans or other corporate planning documents.
- Engage the departmental outreach and communications groups. They can provide valuable insight and advice on outreach activities and can coordinate these efforts with any other related communications initiatives for maximum impact.
- Explain the benefits of online services to clients. Making clients aware of the time-saving and potentially cost-saving benefits of online services provides incentive to use online channels over other channels that are less efficient.
- Ensure that the organization's online services are secure and working properly. Doing so will increase the likelihood that those who use online services have a positive experience and return in the future. It can take only one negative experience for clients to choose not to use the organization's online services, and possibly other government online services. Refer to subsection 4.6 of this guideline for other considerations related to cyber security.

- Limit services exposed and information exchanged to the minimum necessary. Refer to subsection 3.6 of this guideline for information about privacy considerations.
- Address a diverse audience. Clients who are already tech savvy will likely migrate to online services as soon as they are aware they exist. However, other clients may need prompting since not all clients can be reached in the same way or through the same communications medium. Use a variety of platforms and methods (by telephone or in person) to raise awareness. Maintain alternate service delivery channels where appropriate so that clients have choices.

Key elements of a user-engagement approach

- **A client-centric multi-platform awareness campaign:** In order to effectively migrate clients to online services, clients must be aware that this option is available and be aware of its benefits. Promoting awareness of the availability of online services should be done through all existing delivery channels, and can include using correspondence or reminders when providing services in person or through the telephone channels. Departments may wish to promote the benefits of using online services, such as the added convenience a service may offer, or the reduced time it would take to complete an application. These benefits may be communicated in real time, while the client is seeking a service through another channel (by telephone or in person).
- **A client-centric approach to online services:** Ease of use is essential to the success of online services. Good user design, followed by clear and thorough explanations on how to access and use available online services, will help increase their use. Instructions and guidance should be tailored to a wide range of clients, taking into account literacy levels, language and other factors.
- **A measurement plan to assess areas of success and weakness:** It is important to know the extent to which clients are using online services. Engaging with users can increase online service uptake.
- **Limitations of online services:** Beyond legal or security considerations, the online availability of services may not be practical from a cost or benefit perspective or because of other considerations such as technical feasibility. A particular intermediate activity of a service may not be available online under specific circumstances. In such cases, other channels may be required. The online availability of services requires taking a client-centric approach, and clients should be given the option to revert to the online channel once an activity that requires a different delivery channel has been completed.

2.4 Real-time application status

2.4.1 Description and associated requirements

Real-time application status refers to information on the current standing of a client's request for a service or product.

Requirement for departments under the directive
The **designated official for service, in collaboration with other officials** as necessary, is responsible for*:* 4.2.1.2 Ensuring that newly designed or redesigned online services provide real-time application status to clients according to TBS direction and guidance.

2.4.2 Why is this important?

Just as some clients expect to be able to complete the government's authenticated external services online from end to end, they also expect to have access to real-time information on the state of their request or application. When accessing government services, clients need the most up-to-date information that will allow them to make behavioural choices about their interactions. Providing such information facilitates openness and transparency of government processes to provide services and contributes to client satisfaction.

2.4.3 Considerations in implementing the requirement

This requirement applies only to a limited number of the departmental services, which can be identified using the following cascading questions:

- What are the departmental services?
- Which of those services are external services?
- Which of those external services require the client to authenticate themselves in order to apply for or receive the service?
- Which services involve a request and a decision?

When providing real-time application status, consider the following key elements:

- a clear process for clients to receive an update or their application status on the department's website
- access to service and action history (date, actions)
- access to any key messages or advisories related to the service

Following are examples of departments that provide application services in real time:

- Veterans Affairs Canada
- Immigration, Refugees and Citizenship Canada

- Agriculture and Agri-Food Canada

2.5 Service inventory

2.5.1 Description and associated requirements

A service inventory is a catalogue of services that provides detailed information based on a specific set of elements (for example, type, channel, client and volume). It contains information, known as data elements, that enables organizations to better know, understand and more strategically manage their portfolio of services.

Requirement for departments under the policy
Deputy heads are responsible for: 4.2.1.3 Approving the department's service inventory and annual updates.

Requirement for departments under the directive
The **designated official for service, in collaboration with other officials** as necessary, is responsible for: 4.2.1.3 Developing and annually updating a departmental service inventory according to TBS direction and guidance.

2.5.2 Why is this important?

When used effectively, a service inventory can be a useful tool to manage services. A service inventory also demonstrates an organization's commitment to transparency and to service excellence. Using a service inventory has several benefits:

- it provides a snapshot of departmental services and related data, which in turn can support strategic management and decision-making
- it can help determine the resources required for service delivery (for example, staffing, facilities, IT and information management)
- it facilitates performance reporting by linking services to internal performance indicators and external service standards
- it supports the identification of opportunities to create efficiencies through consolidating and standardizing services or the constituent activities or processes within the department and across the Government of Canada

Individual departmental service inventories:

- can be updated via the Government of Canada Service Inventory data collection tool
- have been available on the Government of Canada's open government portal annually since July 2018

Publishing service inventories annually supports a departmental data-driven culture that is open and transparent.

2.5.3 Considerations in implementing the requirements

Identifying services

As a first step, departments can review their annual Departmental Report, Program Inventory and website to identify a list of the department's services. Services could include typical external services that most departments offer, such as public enquiries and access to information requests. Once a list of potential services is established, use the Service Identification Tool described in Appendix B of this guideline to confirm whether the activities undertaken are indeed services. You can also refer to the definition of services in Appendix B to and to the instructions below on developing a service inventory. After this assessment, if your department concludes that it doesn't provide any services, it must submit a declaration from the deputy minister to TBS that indicates the following:

- the department does not offer any services, as defined by TBS direction and guidance
- the department understands that the public-facing GC Service Inventory will show that the department does not offer any services

This declaration can be revisited regularly, and the organization should notify TBS when the declaration is no longer accurate, or upon TBS's request.

Best practices for developing a service inventory

- Prepare to develop a service inventory:
  - identify a champion at the senior management table
  - identify a departmental lead or coordinator
  - identify key contributors in the department (branches/sectors)
  - develop a plan with key activities and timelines
  - convene an information session with contributors to kick off data collection within the organization
- Develop a service inventory
  - read the *Policy on Service and Digital*, the *Directive on Service and Digital* and related policy instruments and guidelines on TBS's website
  - review the Service Identification Tool (see Appendix B of this guideline)
  - verify for any updates on the directive or guidance from TBS
  - review your Departmental Plan, Program Inventory and website to prepare a draft list of services
  - work with departmental partners to confirm services and related data elements
  - become familiar with TBS's data collection website to ensure that data collected aligns with the data fields required
- Post-development of a service inventory:
  - seek approval from your deputy head and information management senior official to allow publication on open.canada.ca

- use the login credentials sent by TBS to access the data collection website
- keep the department's service inventory evergreen by updating it regularly

Key components of a service inventory

A service inventory includes a number of data elements, such as the following:

- service name
- service type
- special designations
- URL to access the service
- link to program inventories
- client type
- volume of transactions
- service standards and related performance information
- use of a business number or a social insurance number
- service fees
- online availability

A service inventory template, which identifies the full set of required data elements and related definitions, can be found on the GC Service Community page.

You will need to input your departmental data via a web-based tool launched by TBS.
Although departments and agencies are required to review data elements in all fields annually, some fields will remain static year over year.
The following are some key points to consider when developing and updating a service inventory:

- The information in a service inventory should be verified and be consistent with data contained in a departmental Performance Information Profile (PIPs) and other planning documents (for example, Departmental Plan and departmental data strategy).
- It is important to keep your service inventory evergreen by updating it on a regular or annual basis. Such updates are essential in order for your service inventory to accurately indicate the services provided by your department.
- It is also important that your department identifies:
  - the custodian(s) of the inventory
  - most recent revision date
  - other important information that can serve as a reference point for those using or managing this information in the future.

Service name considerations

When naming a new service or revising an existing service name, consider the following:

- be concise and use plain language

- use names that are easily identifiable and relevant to the clients it serve (for example, “Call Centre,” “Complaints”)
- avoid using acronyms as part of the service name
- ensure that the service name is consistent with names used in the departmental or Canada.ca website and departmental reports, including “service inventory”
- avoid labelling the service with the name of a branch or sector, unless necessary
- avoid including the words “process,” “program,” “service” or “activity” in the service name, unless required to align with a legislated or policy requirement

2.6 Availability of service inventory on the open governmental portal

2.6.1 Description and associated requirement

The *Directive on Service and Digital* requires departments to make their service inventory available through the Government of Canada Service Inventory, a consolidated database of Government of Canada services and related performance information open to the public via the open government portal.

Requirement for departments under the directive
The **designated official for service, in collaboration with other officials** as necessary, is responsible for*:* 4.2.1.4 Working with TBS to make the departmental service inventory available through the Government of Canada open government portal according to TBS direction and guidance.

2.6.2 Why is this important?

The requirement to have departmental service inventories on the open governmental portal:

- provides open and transparent access to Government of Canada service information to departments, central agencies, academia and the public
- facilitates government-wide performance reporting
- supports the Government of Canada strategic management and decision-making

2.6.3 Considerations in implementing the requirement

As specified in the *Directive on Service and Digital*, the designated official for service, in collaboration with other officials as necessary, is responsible for:

- ensuring that service inventory data submitted to TBS is accurate
- working with TBS to revise the departmental service inventory for government-wide consistency for the purposes of release on the open government portal

Departments remain responsible for the accuracy of their data, and TBS is the custodian of the service inventory data for publishing purposes.

Timing

Although departments can update their service inventories at any time, they will typically collect data for the previous fiscal year during the summer, in time for TBS's review and publishing on the open government portal in the fall.

Link to other requirements and policies

Service inventories must link to other requirements and policies, including:

- requirements 4.3.2.8 and 4.3.2.9 of the *Policy on Service and Digital* to release information and data on the open government portal (refer to subsection 3.4 of this guideline for more information)
- subsection 6.2 of the *Directive on Open Government*, which requires that open data and open information is released in accessible and reusable formats via Government of Canada websites and services designated by TBS
- the *Policy on Results*

2.7 Service standards

2.7.1 Description and associated requirement

A service standard is a public commitment to a measurable level of performance that clients can expect under normal circumstances when requesting a service. The term "normal circumstances" refers to the expected level of supply and demand for regular day-to-day service operations. Such operations differ from special circumstances where regular service standards may not apply (for example, circumstances that are typically not within the organization's control, including holidays, natural disasters or other emergency situations).

Requirement for departments under the policy
Deputy heads are responsible for: 4.2.1.4 Ensuring services have comprehensive and transparent client-centric standards, related targets, and performance information, for all service delivery channels in use, and this information is available on the department's web presence.

2.7.2 Why is this important?

Service standards reinforce government accountability by making performance transparent. They also increase the confidence of Canadians in government by demonstrating the government's commitment to service excellence. They are integral to good client service and to effectively managing performance, and can clarify expectations for clients and employees, drive service improvement, and contribute to results-based management. Service standards also help clients make time-sensitive, important decisions about accessing services and other expectations relating to services.

2.7.3 Considerations in implementing the requirement

Key components of this policy requirement include the following:

- scope: applies to all services where there is a clear and specific recipient
- channels: service standards must be developed for all service delivery channels, as applicable (for example, in person, telephone and online)
- comprehensiveness: includes access, timeliness, accuracy and real-time performance

- consistency: proposes a common approach to articulating standards and measuring their fulfillment
- transparency: focuses on what, how, where and when to publish information

In addition to this policy requirement, departments must consider other service standard requirements in other policy instruments, Acts of Parliament and regulations to ensure alignment. Examples are:

- *Policy on Transfer Payments*
- *Service Fees Act*
- *Directive on Charging and Special Financial Authorities*
- *Cabinet Directive on Regulation*
- *Canada.ca Content and Information Architecture Specification*

In order to develop comprehensive service standards, departments consider the three types of standards:

1. Access standard: a commitment outlining the ease and convenience the client should experience when attempting to access a service (for example, the likelihood that callers will be able to speak with an agent, hours in a day that the service can be accessed)
2. Timeliness standard: a commitment stating how long the client should expect to wait to receive a service once the service has been accessed (for example, how long callers will have to wait to speak with an agent once they are in the queue)
3. Accuracy standard: a commitment stipulating that the client will receive a service that is up-to-date, free of errors and complete (for example, will callers receive the correct answers to their questions)

Service standards typically have three key components:

1. Service standard: a clear and measurable statement on the level of service a client can expect (for example, answer calls within 20 seconds or process applications within five business days)
2. Service performance target: a clear and measurable statement on the extent (frequency) to which (in terms of percentage) the standard will be met (for example, “we will meet our service standard 95% of the time”)
3. Service performance result: the actual performance against the standard target (for example, “we met our target 96% of the time”), typically reported on an annual, quarterly or monthly average

Refer to the table in subsection 2.9 of this guideline for examples of service performance metrics.

Characteristics of a good service standard

When designing or reviewing service standards, consider the following key characteristics:

- Relevance to the client: service standards are consistent with client expectations and address aspects of the service they value most within available resource allocations.
- Simplicity: service standards are easy to understand and address only one dimension of performance.

- Based on consultations: service standards are developed or reviewed in consultation with clients, managers, staff and other partners in service delivery to ensure that they are meaningful to clients and match the organization's mandate and capacity. Note that the *Service Fees Act* requires that mandatory consultations be undertaken before modifying a service standard.
- Measurable: service standards are quantifiable and linked to monitoring activities.
- Consistent across government: service standards should be consistent throughout departments that provide similar services. Having similar service standards across government for similar services helps both clients and government. Clients will find it easier to deal with different organizations, and the organizations themselves will find it easier to share best practices and adopt common approaches.
- Ambitious but realistic: service standards are sufficiently challenging to service providers yet are realistic in terms of capacity.
- Endorsed by management: Service standards are understood and endorsed by senior management.
- Communicated: service standards are clearly communicated to clients, employees and other stakeholders to help manage expectations and performance.
- Transparent: service standards are monitored and reported to senior management, and performance results are made available on their web presence to ensure transparency and promote client trust.
- Continually updated: service standards are regularly reviewed and updated as appropriate.

In addition to the service characteristics described above, when establishing service standards, consider the following:

- Secure the necessary approvals for proposed service standards and operational targets. From the outset, determine which level of approval is required before implementing a service standard and an operational target. Some service standards are established in policy or legislation and may require ministerial approval. Involving legal affairs from the outset can also identify and mitigate potential challenges early in the approval process.
- Explore the implications of national (or global) service standards on regional services. Departments that deliver services across the country (and, in some instances, worldwide) may wish to consider the targeted client groups and the different resource levels at each service point. Determining the impact of national standards on regional operations before implementation can address potential variations and implementation challenges. National service standards are preferred because they help departments communicate a consistent message to all clients. Where possible, avoid sending different messages to each region or client group or encouraging unwanted comparisons between the levels of service offered in each region.

- Verify that service standards do not create legal liabilities. Involve your department's legal services unit early in the process and consult on the wording of service standards and the potential risks associated with non-performance. Fine print, footnotes and other forms of caveats may provide good risk management, but be careful not to overly diminish the intent of service standards or to create readability or interpretation challenges for clients.

The following are some best practices when developing service standards:

- avoid identifying a performance target within the service standard
- for the timeliness of service standards, use number of weeks, business days or hours, as appropriate
- do not use time ranges in service standards (for example, "between X and Y business days")
- in special circumstances, timelines may be negotiated on a case-by-case basis (for example, respond to media enquiries within timelines negotiated between the two parties)
- ensure that the service standards and related performance information reported on your department's web presence is consistent with the information provided in your departmental service inventory

2.8 Review of service standards

2.8.1 Description and associated requirement

Once service standards have been developed, they should be regularly reviewed and improved to ensure that they are comprehensive, meaningful and relevant.

Requirement for departments under the directive
The **designated official for service, in collaboration with other officials** as necessary, is responsible for: 4.2.1.5 Ensuring the development, management and regular review of service standards, related targets and performance information, for all services and all service delivery channels in use, according to TBS direction and guidance.

2.8.2 Why is this important?

The process of reviewing service standards is important to ensure that they are comprehensive, consistent and meaningful to Canadians. Reviewing service standards helps identify any gaps or areas for improvement and courses of action to address key gaps in performance.

2.8.3 Considerations in implementing the requirement

The following Service Standards Development and Assessment Tool can help departments review their service standards. The table below provides a series of questions that organizations can answer. If the answer to a question is yes, indicate your data or evidence source in the adjacent column. If the answer to a question is no, this may indicate a gap that would need to be addressed.

Questions	Considerations	Yes, no or n/a	Evidence or data source
1. Are the service standards comprehensive in perspective?	Service standards should address different aspects and channels (for example, in person, telephone and online) of service delivery, as appropriate.		
a) Is there an access standard?	Service standards should outline a commitment for the ease and convenience the client should experience when attempting to access a service.		
b) Is there a timeliness standard?	Service standards should outline a commitment stating how long the client should expect to wait to receive a service once the service has been accessed.		

Questions	Considerations	Yes, no or n/a	Evidence or data source
c) Is there an accuracy standard?	Service standards should outline a commitment stipulating that the client will receive a service that is up-to-date, free of errors and complete.		
2. Do the standards align with client needs and expectations?	Service standards should take into consideration the needs and expectations of clients. Such consideration is a key element of public opinion research and consultations with clients, and helps ensure that standards are meaningful to clients.		
3. Are the service standards based on consultations with various stakeholders?	Service standards should be developed and updated in consultation with clients, managers, staff and other stakeholders in service delivery.		
4. Are the service standards measurable?	Service standards should be quantifiable and linked to broader performance monitoring activities.		
5. Do the standards align with specific requirements contained in applicable legislation and policies?	Service standards should meet specific provisions as articulated in legislation and policy (where applicable) (for example, the *Policy on Transfer Payments*, the *Service Fees Act*, the *Directive on Charging and Special Financial Authorities*, the *Cabinet Directive on Regulation* and associated policies and guidance documents).		
6. Are the service standards consistent with those of similar services?	Similar services offered by various programs, departments and jurisdictions should have similar standards where appropriate. Clients will find it easier to deal with different organizations, and the organizations themselves will find it easier to share best practices and adopt common approaches.		

Questions	Considerations	Yes, no or n/a	Evidence or data source
7. Are the service standards realistic (for example, reasonable and practical)?	Service standards should be sufficiently challenging to service providers yet attainable in terms of resources and overall departmental capacity (that is, operational capacity, business processes or systems) to meet the standards.		
8. Are the service standards endorsed by management?	Service standards should be understood and endorsed by senior management.		
9. Are the service standards and related performance results available to staff, management, clients and stakeholders?	Service standards and related performance results should be available to employees, senior management, clients and other stakeholders to help manage expectations and performance.		
10. Have the appropriate web publishing and templates been used to communicate service standards, targets and related performance results online?	Service standards, current status and performance reporting should be presented online clearly, simply and consistently so that citizens and clients know what to expect when accessing a service.		
11. Have the service standards been reviewed and updated within the service review period (every five years)?	Service standards should be regularly reviewed and updated using this tool and within the period of the service review, or sooner, as appropriate. See subsection 2.10 of this guideline for more information about service review.		
12. Is real-time performance information related to service standards being published?	Real-time service performance information should be linked to service standard targets.		

When reviewing service standards, consider the following.

Find the right balance between ambitious and safe standards

Establishing ambitious but achievable standards helps an organization improve its performance and meet the expectations of clients. Reviewing service standards regularly and taking performance into account provides an opportunity for adjustment, including raising the standards if appropriate. Organizations that strive to continually improve their performance are likely to meet client expectations more frequently and thereby increase client satisfaction. After service standards have been in place for a while and have matured (that is, they are meeting their performance over 95% of the time), departments may decide to review and improve them. Increases in expectations should be gradual to ensure that employees understand the changes and can contribute to their attainment.

Clients gain confidence in the government when standards are met consistently. Departments are encouraged to allocate resources to meet any new improved service levels.

Monitor performance to determine whether course corrections are required

A regular review of whether service standards and operational targets are being met can help senior managers determine whether resource adjustments are required. It is possible that the service standard may be overly ambitious or set too low.

Determine whether the variance between the service standard and actual performance is temporary or long-standing. It may be necessary to scan the environment, internally and externally, to determine possible influences that affect the attainment of service standards.

The table below identifies three performance results scenarios and possible courses of action.

Performance results scenarios

Scenario 1: **Performance results exceed service standard target**	**Scenario 2:** **Performance results are consistent with service standard target**	**Scenario 3:** **Performance results fall short of service standard target**
1. Determine why standards are being exceeded: • Was the methodology used to develop the standards adequate? • Has the organization's capacity improved? • Are the standards too low? • Were projections about trends and client behaviours accurate? • Did circumstances change, such as lower-than-expected demand or new delivery approaches? 2. Decide how to respond: • Raise standards where appropriate. • Redeploy resources to lower-performing areas. • Communicate results to clients, staff and service delivery partners. • Share knowledge, including best practices and lessons learned, with the service community. • Celebrate success. 3. Plan to address emerging or longer-term issues, such as resources, capacity, expected change in demand and new priorities.	1. Confirm whether clients are satisfied with current levels of service through client feedback and results of client satisfaction measurement. 2. Determine whether higher standards are warranted or desirable. 3. Plan to address emerging or longer-term issues such as resources, capacity, expected change in demand and new priorities.	1. Determine why standards are not being met: • Are service standards too high? • Is the business process unclear or unnecessarily cumbersome? • Were there unexpected changes in resource capacity and level of demand for service? • Was sufficient attention paid to the potential impact of known trends, such as new demand, or change in channel preferences? 2. Decide how to respond: • Rethink the business process? • Increase capacity? • Identify and implement best practices for similar services? • Consult stakeholders? • Lower service standards, if appropriate? 3. Inform stakeholders of your plans to address outstanding issues and to improve service. Remember to take financial resources and changing organizational priorities into account.

2.9 Real-time service performance information

2.9.1 Description and associated requirement

Real-time performance information relates to the current level of performance that clients can expect to be provided for a service, relative to an established standard.

The concept of "real time" means that timely information on the expected delivery of the final (service) output is available so that citizens and businesses can choose when to use government services based on that information. For example, travellers approaching Canada can check the Canada Border Services Agency's online service to know the current wait times at a particular border crossing and decide on which to use. In publishing this information, the Canada Border Services Agency helps clients set realistic expectations about its service.

Real-time service delivery performance information can be grouped into three categories based on the frequency of updates and the speed in which information is processed. They are as follows:

1. Timed updates: service delivery performance information is made available to clients based on timed or scheduled events (for example, once a month, week, day or hour, as appropriate)
2. Near real-time updates: service delivery performance information is made available to clients within a minimal delay (for example, a 5-minute delay)
3. Instantaneous updates: service delivery performance information is made available to clients immediately and without delay (for example, live information feed)

In all cases, it is important to include information related to the frequency of updates and the date or time of the latest update.

Requirement for departments under the directive
The **designated official for service, in collaboration with other officials** as necessary, is responsible for: 4.2.1.6 Ensuring the reporting of real-time performance information for service standards is available on the department's web presence, in accordance with TBS direction and guidance.

2.9.2 Why is this important?

Although service standards inform clients about what to expect based on service performance targets, they do not provide current performance information that permits citizens and businesses to make behavioural choices when accessing government services. Real-time service delivery performance information bridges this gap.

2.9.3 Considerations in implementing the requirement

Determining the best approach to publishing real-time performance data

Before determining the best approach to publishing real-time performance data, determine what is affordable given the operational context. A cost-benefit analysis or other type of analysis that determines whether the benefit outweighs the implementation cost is recommended. Undertaking such an analysis provides senior managers with the information necessary to determine the best approach given the operational context.

The frequency and speed of updates may vary for each service depending on the type of service and context of its delivery. Departments need to:

- consider what real time means in the context of each service, including what makes sense to clients
- determine how best to publish real-time service delivery performance information

Service providers are best positioned to determine which frequency of update is most suited to each service.

Typically, real-time information is focused on the timing to deliver a final output to a client. It can, however, provide updates on the anticipated time frames for delivering intermediate outputs if they are anticipated by, and given directly to, clients as part of a larger process to deliver a service.

Departments and agencies should ensure that this information is easily accessible on their web presence and through any other channel of service delivery, as appropriate.

When establishing real-time service delivery performance information approaches, consider the following key characteristics:

- easily and quickly accessed
- relevant to the client
- linked to service standards
- communicated
- transparent
- timeliness and accuracy of data
- focused on outputs, that is, whether on the final (service) output or an intermediate output

Publishing service standard information

There are two perspectives when publishing service standard information:

1. by service: for each service, the following would be indicated:
    - service name
    - description
    - application steps
    - service standard and target
    - real-time performance information
2. through performance reporting: for each service, the following would be indicated:
    - service name
    - service description
    - service standard

- target
- annual performance for the most recent year data available

Note that real-time service performance information can be published on the service page or in a central location on the organization's web presence that is easily accessible from the service page.

To facilitate online publishing of service standards information in both of these contexts, templates and patterns are available in the Canada.ca design system:

- for in-service scenarios, see the template for Service initiation page: Canada.ca template
- for performance reporting, see the template for Institutional service performance reporting page: Canada.ca template

When publishing service standards, do so in a way that is simple and clear to people using the service, and assess their accessibility through usability testing. In addition, when providing real-time performance information, it is important to include the frequency of updates and the date and time of the last update.

Understanding how different service performance metrics link together

Four distinct and complementary metrics are as follows:

1. service standards
2. performance targets
3. real-time service delivery information
4. performance targets and average service performance information

Departments can use these metrics together to help manage service delivery results and client expectations.

The table below provides examples of the different metrics used to assess service performance.

Examples of service performance metrics

Service standard	Service standard performance target	Real-time service performance information	Average service performance result
Applications are processed within 60 days.	The target for achieving this standard is set at 90%.	Currently processing applications within 45 days as of (date). Updated monthly as of this date.	The service standard was met 91% on average in fiscal year XX.
Issue a claim payment cheque within 15 business days of receiving a complete claim from the client, including all of the required claim information.	The target for meeting this standard is set at 95%	Currently issuing claim payment cheques within 10 days of receiving a complete claim as of (date). Updated weekly as of this date.	The service standard was met 89% on average in fiscal year XX.

Service metrics portfolio

Managers can monitor service performance over time by collecting data on:

- implementing service standards
- attainment of performance targets
- performance information

The data can be analyzed to improve an individual service and better manage services across a service metrics portfolio.

A service metrics portfolio can represent all the service metrics a department has in place or represent a common set of services. Examining service metrics across a portfolio increases transparency and encourages consistency. It also facilitates the development of coherent approaches to implementing and using metrics across sectors and branches. Finally, examining service metrics as a portfolio helps ensure that all major services and client groups have been addressed.

When integrated with corporate planning and reporting activities, service metrics are a useful tool to support overall organizational management:

- The Treasury Board *Policy on Results* requires departments to establish a Performance Information Profile. Service standards and real-time performance information comprise two sources of information that can be used to develop a performance measurement framework related to services.

  Part III of the Estimates process requires that departments prepare departmental expenditure plans consisting of Departmental Plans and Departmental Results Reports, service standards and related performance information help express and formulate performance objectives and can be incorporated into the business planning process. Reporting on performance against service standards helps demonstrate progress toward expected results.
- The Management Accountability Framework (MAF) sets out the Treasury Board's expectations for effective performance. One of the several elements that make up the MAF is service management. Service standards and related performance information are essential components in achieving service excellence and directly contribute to advancing results-oriented management activities**.**

Planning for success

If a department is in the early stages of implementing service standards, it is encouraged to develop an implementation plan to enable compliance with all existing mandatory requirements related to service standards. Additionally, such a plan could be considered as a service improvement initiative or project for inclusion in the department's overall service improvement plan.

Service agreements

A service agreement is a formal administrative understanding between two or more parties that articulates the terms and conditions of a particular service relationship between two or more parties. Establishing service agreements is a sound management practice in any type of service owner or service provider arrangement when, for example, a Government of Canada service is provided by one department to, or on behalf of, another department.

Service agreements can enhance governance, accountability and service quality by clearly defining roles, responsibilities, processes and performance expectations. The practice of establishing service agreements is strongly recommended for any type of service owner, service provider or collaborative service relationship. Aspects of the service relationship that are typically documented in a service agreement include scope, governance, operations, finances, performance and implementation.

Service agreements serve three primary functions:

1. articulate the expectations of the parties to the agreement
2. provide a mechanism for governance and issue resolution
3. act as a scorecard against which to examine performance and results

For additional information and tools for this aspect of service management, consult the two TBS guidelines on service agreements:

- the *Guideline on Service Agreements: An Overview* provides an overview of service agreements and is geared toward senior managers and executives
- the *Guideline on Service Agreements: Essential Elements* describes the essential elements of these agreements and is intended for individuals responsible for developing or reviewing service agreements

For service agreements that involve personal information, refer to *Guidance on Preparing Information Sharing Agreements Involving Personal Information*.

2.10 Service review

2.10.1 Description and associated requirements

A review of services consists of a systematic assessment of an organization's services against a set of predetermined criteria to identify opportunities for service improvement, including greater effectiveness and increased efficiency.

Requirement for departments under the policy
Deputy heads are responsible for: 4.2.1.5 Ensuring that services are reviewed to identify opportunities for improvement.

Requirement for departments under the directive
The **designated official for service, in collaboration with other officials** as necessary, is responsible for: 4.2.1.7 Ensuring that each service is regularly reviewed with clients, partners and stakeholders, in collaboration with the departmental CIO, as appropriate, at least once every five years to identify opportunities for improvement, including redesign for client-centricity, digital enablement, online availability and uptake, efficiency, partnership arrangements, and alternate approaches to service delivery.

2.10.2 Why is this important?

The regular review of services is a key practice in ensuring that services:

- meet the evolving needs and expectations of clients
- are efficient
- align with the overall Government of Canada service direction

By systematically reviewing its services, the Government of Canada can improve its business processes, achieve efficiency gains, and strive for greater client-centric services.

2.10.3 Considerations in implementing the requirements

A departmental review of services does not need to be complex, but it does require the following:

- a methodical approach
- good understanding of the organization's current service environment, its priorities and its services
- coordination with key departmental and other service stakeholders

When undertaking a review of services, consider the following steps:

1. Identify or establish a working group of representatives from various areas within your department that have an interest or stake in this exercise. Consider including key

representatives from the policy, program, service delivery, information management, IT, security, privacy and corporate/strategic planning areas of your department.

2. Identify and confirm your department's services, referring to your departmental service inventory.
3. Develop a five-year plan that incorporates all departmental services and that identifies which services will be reviewed in each year. Keep this plan evergreen by updating it annually to reflect changes in services or review priorities.
4. Identify and confirm the key review questions that will be used to assess your department's services. Apply the key review questions (below) to assess the departmental services identified for review in the given year.
5. For services that are identified as having potential for redesign or optimization, identify the specific improvement initiatives that are required. For each potential redesign or optimization initiative, consider the following questions:
   a) What are the overall benefits?
   b) What are the associated costs?
   c) What are the risks of proceeding or not proceeding?
   d) Are there opportunities to collaborate with others?
   e) Can knowledge gained from experimentation be leveraged?
6. On the basis of Step 4, identify which services should be recommended for service redesign or optimization and establish a draft implementation plan with key actions, project leads and timelines. Also consider collaborating with key organizational partners in service delivery, such as program managers, the departmental CIO, communications representatives and other departmental officials, as appropriate.
7. Validate the proposed service redesign and optimization implementation plan with your organization's senior management. When appropriate, engage in broader discussions with potential external service delivery partners (such as other departments or jurisdictions that have similar mandates, services or business processes) and clients.
8. Once approved, the service redesign and optimization initiatives should be reflected in your department's key planning documents, such as a service improvement plan and the required integrated plan, as appropriate. Refer to subsection 1.3 of this guideline for further details on integrated planning.
9. Regularly monitor the implementation of the plan and report on progress. Ensure appropriate linkages to your department's planning documents, performance measurement framework, and any other government-wide service improvement initiatives.
10. Review and adjust your plans as required, ensuring that your service improvement initiatives address the needs of your clients and result in operational efficiencies.

Key review questions

Once you have identified your overarching goals or objectives for service improvement, you may wish to consider the following **key review questions** as part of your review of services.

1. Are there any specific client satisfaction issues related to the department's services that need to be addressed? A review of performance against service standards, the results of recent audits, evaluations, surveys of client satisfaction and media articles is a good place to start.
2. Are there any opportunities to make the service more client-centric? Consider the following key service elements: client-centric service by design, including access, inclusion, accessibility, security, privacy, simplicity and choice of official language.
   In addition, you may wish to consider the following elements:
   - choice of service access point
   - ease of access ("findability")
   - seamless and integrated
   - streamlined and intuitive application process
   - consistency in experience
   - proactive delivery
3. Is the service obtained through digital enablement?
4. Are any of the department's services not available online, end to end? If not, why is this the case, and can these services be modernized to meet the online service expectations of clients? What is the uptake rate of online services relative to those offered through other channels (telephone or in person), and what can be done to improve the uptake if required?
5. Are there opportunities to improve the efficiency of service delivery? Consider the following:
   - streamlining business processes
   - managing service channels to increase the number and use of online services and reduce the volume of more expensive in-person and telephone services (incentives and disincentives)
6. Are there opportunities to align or integrate services or service improvement initiatives with others (within the program, department, government or other jurisdictions)? Are there better ways to deliver the service through partnerships with the private sector or by leveraging artificial intelligence?

3. Open and strategic management of information

Every day, departments generate and collect large volumes of information and data as they carry out their work. This information and data support a wide variety of programs and activities, including transactions, operations, decisions, services, communications and reporting exercises. Departments need reliable information and data to function effectively and provide evidence to support the actions and decisions of public officials. To deliver on their mandates and maintain transparency and accountability, departments need to ensure that they are:

- actively managing and protecting their information and data holdings
- meeting legal obligations to protect privacy and confidentiality and provide access to government records to Canadians

As the currency of digital government, information and data are strategic assets that play an increasingly central role in the decisions and operations of departments, as well as in designing and delivering services to citizens and businesses. In order for information and data to be effectively leveraged to improve services for Canadians, they must first be well managed. This section of the guideline, which is for deputy heads, departmental CIOs, managers and employees, describes best practices and recommendations on managing information and data strategically.

Treating information and data as strategic assets involves dedicating resources in order to:

- ensure that information and data management initiatives are in line with business objectives and legal obligations
- put in place the tools and systems needed to manage information and data effectively throughout their life cycle

The management of information and data is never an end in itself; it is always intended to support actions or inform decisions within an organization. Departments must know what information and data they possess, and understand their value, in order to use and safeguard that information and data effectively in the organization's decision-making processes.

In the digital age, robust information and data management practices are increasingly crucial because they:

- support effective departmental operations, delivery of services, and accountability to the public
- underpin various legal obligations such as privacy requirements, the public's right of access to government information, the proactive release of government information online, and the long-term preservation of Canada's documentary heritage

Among the expected outcomes of the *Policy on Service and Digital* is that information is managed as a strategic asset, throughout its life cycle, and is increasingly open to enable interoperability and transparency.

Refer to Appendix C of this guideline for a definition and description of the terms information and data, in the context of the *Policy on Service and Digital* and the *Directive on Service and Digital*.

3.1 Strategic management of information and data

3.1.1 Description and associated requirements

The main focus of this theme is how to manage information and data as strategic assets. Managing strategically involves ensuring that deputy heads invest in the rules, tools and people needed to govern and manage information and data throughout the various stages of their life cycles.

Requirements for departments under the policy

Deputy heads are responsible for:

4.3.2.1 Ensuring that information and data are managed as a strategic asset to support government operations, service delivery, analysis and decision-making.

4.3.2.2 Ensuring that methodologies, mechanisms and tools are implemented to support information and data life cycle management.

4.3.2.3 Ensuring that departmental responsibilities and accountability structures are clearly defined for the management of information and data.

4.3.2.10 Ensuring that decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of how policies and programs have evolved, support litigation readiness, and allow for independent evaluation, audit and review.

The corresponding requirements in the *Directive on Service and Digital* lay out the responsibilities of the departmental CIO, managers and employees with respect to:

- the duty to document activities and decisions of business value
- the holistic management and governance of information and data, including creation and collection, use and reuse, and disposition

Requirements for departments under the directive

The **departmental CIO** is responsible for:

4.3.1.6 Documenting life-cycle management practices within the department that align with the nature or purpose of the information or data, and that address accountability, stewardship, performance measurement, reporting, and legal requirements.

4.3.1.7 Establishing, implementing and maintaining retention periods for all information and data, as appropriate, according to format.

4.3.1.8 Developing a documented disposition process and performing regular disposition activities for all information and data, as required.

4.3.1.10 Identifying information of business value, based on an analysis of the functions and activities carried out by a department to enable or support its legislated mandate.

4.3.1.11 Maximizing the removal of access restrictions on departmental information that has been identified as having archival value before the information is transferred to Library and Archives Canada as part of planned disposition activities.

4.3.1.12 Ensuring that an approved Government of Canada enterprise information management solution is used to document business activities, decisions and decision-making processes.

4.3.1.13 Identifying, establishing, implementing and maintaining designated corporate repositories in which information of business value is managed throughout its life cycle while respecting privacy and security requirements.

4.3.1.14 Ensuring that the quality of information is managed and preserved to satisfy the requirements and expectations of users to meet operational needs, responsibilities, and long-term retention requirements.

Managers are responsible for:

4.3.2.1 Informing employees of their duty to document their activities and decisions of business value.

Employees are responsible for:

4.3.3.1 Documenting their activities and decisions of business value.

The life-cycle stages of information and data are largely consistent across varying organizational contexts. They generally concern creation and capture, management, use and sharing. At each of these key stages, it is recommended that departments manage and govern data in a responsible manner that:

- enables interoperability
- assures fitness for purpose
- maximizes accessibility and discoverability
- respects relevant security, privacy and other legal obligations, in accordance with applicable laws and policies

In addition, periodic assessment of the value and utility of information and data can help inform approaches to retention and disposition. It can also ensure that departmental resources are allocated to the information and data deemed most valuable and useful to departmental objectives and whole-of-government priorities, such as improved government operations and services.

3.1.2 Why is this important?

Information and data are foundational elements of digital government. The Government of Canada aims to be a more open and user-centric provider of programs and services to people and businesses in simple, modern and effective ways that are optimized to be available anytime and anywhere, from any device.

To realize this vision, which captures the way Canadians increasingly expect to interact with government, information and data held by the government should be viewed and treated as an asset that is similar to finances or real property, both at the departmental and enterprise levels. Adopting a standard approach to the strategic management of information and data at the departmental level helps create the digital environment needed to enable accessibility, discoverability, shareability, and interoperability at the enterprise level. Using a standard approach also enables greater openness, transparency and accountability to the Canadian public.

Currently, there is significant variation in the level of data maturity of departments, as evidenced by their data strategies. In areas such as quality, architecture, ethics and accountability, information and data are managed in an ad hoc manner. This fragmented digital environment lacks consistency in information and data across systems and limits interoperability among them. And given the lack of a comprehensive view of government-held information and data, weak levels of standardization also lead to redundant information and data collection, which negatively impacts the efficiency and effectiveness of government operations, as well as the government's ability to deliver evidence-informed decisions and digitally enabled services to Canadians.

Taken together, these challenges form the rationale behind the theme of managing information and data strategically, as it is primarily intended to strengthen the capacity of departments to adopt existing and emerging enterprise-wide information and data standards. It is expected that the standardization of information and data management and governance practices will enable the federal public service to realize the service delivery model that citizens and businesses increasingly expect, while maintaining government accountability.

3.1.3 Considerations in implementing the requirements

Mandatory Procedures for Enterprise Architecture Assessment (Appendix A of the *Directive on Service and Digital*) provides enterprise architecture requirements to help ensure that information and data life-cycle management practices are aligned across government.

In addition to these requirements, the following points lay out a set of best practices and considerations for each stage of information and data life-cycle management (creation and collection, management, use and sharing). It is recommended that departments incorporate them into their implementation plans (for example, for their departmental data strategies or, in the long term, their integrated departmental plans) or use them to supplement existing rules, methodologies, mechanisms or tools in this area. Best practices and considerations seek to help departments achieve several key outcomes:

- improved understanding of currently held information and data assets, including identifying personal information holdings
- clearly defined roles and responsibilities for information and data assets, addressing accountability for the use or misuse of these assets
- increased capacity to identify, recognize and manage information and data with business value and determine eligibility for release as open data and information in accordance with applicable laws (see Appendix C of this guideline)
- regularly assessed schedules and processes for the retention and disposition of information and data assets, in accordance with the requirements of the *Privacy Act*, other relevant legislation or policy, and Library and Archives Canada's disposition authorizations

1. Information and data creation and capture

Plan for information and data needs. Consider the following questions when thinking about the information and data needed to accomplish business objectives and make evidence-informed decisions:

- What type of information and data are needed to support or inform work objectives, and how will they be accessed or captured? The performance indicators in a program's Performance Information Profile (PIP), as laid out in the *Policy on Results* (subsections 4.3.5 to 4.3.7), can help determine these needs.
- Are any published information and data (for example, structured data such as a relational database, unstructured data such as books, reports, articles or other online resources, and semi-structured data such as XML and JSON) needed? (See Appendix C of this guideline for more details on the distinction between information and data.) If so, how will access to this information and data be sought in a way that minimizes costs and avoids duplication?
- Is it possible that any information and data needed may have already been captured by another department? If so, how will access to and reuse of this information and data be sought in order

to minimize redundancies, avoid duplication and ensure compliance with the *Privacy Act* and other relevant policy or legislation?

- Will any of the information and data planned to be captured or created require security classification? If so, at what level(s)?
- Do you have the authority to capture personal information and data? Have you identified the purpose of the capture?
- Has a Privacy Impact Assessment been performed, or is it needed to address any privacy issues or risks associated with the information and data that will be captured or created? Have you registered a new or is there currently an existing Personal Information Bank (PIB) and class of personal information that describes:
  - the purposes for which the department is capturing the personal information?
  - the privacy practices that support the administration of programs and activities?
- What steps are you taking to mitigate security, privacy or other legal risks at the outset of capturing the information or data in order to support an "open by design" approach and improve readiness to release information and data to the open government portal (as set out in subsection 4.3.2.8 of the policy)?
- What steps are you taking to ensure that information or data captured is, or can be, disaggregated to the lowest relevant administrative level (for example, sex and gender, ethnicity, geographical location)? Refer to the policy direction to modernize the Government of Canada's sex and gender information practices.

As information and data are created and captured, identify its organizational, enterprise and public value and manage it in a way that maximizes its availability to those who need it or request it through formal or informal channels. To this end, the following practices are recommended:

- Use digital systems to create, capture, manage, use and share information and data. Refer to subsection 3.2 of this guideline for more information on the use of digital systems. Ensure that the systems used for the creation and capture of information and data:
  - allow for the management and maintenance of records over time
  - support import, export and interoperability
  - maintain adequate context through metadata
- For common information and data domains, ensure alignment with enterprise-wide information and data standards, as appropriate. Follow departmental conventions for naming, metadata and classification when creating and organizing all other information and data.
- In order to have an accurate and complete picture of the government's decisions and actions, it is every individual employee's responsibility to document the relevant information and data that provides evidence in support of actions and decisions taken within the context of government

business (duty to document). This duty also involves documenting and tracking the purposes for which information and data are collected or used.

- Exercise the duty to document by identifying information and data of business value and ensuring that these are captured and stored in a designated corporate repository, such as an Electronic Documents and Records Management Solution (for example, GCdocs), as appropriate (see Appendix D of this guideline for more information about business value):
    - A designated corporate repository is an information storage repository that departments authorize for managing information and data of business value. In making this designation, the organization takes responsibility for:
        - keeping that repository operational during business hours
        - performing backup and other safety measures
        - applying the appropriate security measures
        - obtaining the appropriate insurance coverage
        - exercising all other prudent asset management practices over the repository
    - Consider carefully what information needs to be documented for the purposes of reconstructing the evolution of policies and programs. Map out and document the process that culminates in a decision, such that the steps of that process and the data, information and evidence used to support it can be traced for audit or other purposes. It is not expected that all of a department's processes be documented. Focus on the key decision-making and policy-making processes that are part of core business or that impact the public.
- Include email and instant messages of business value when storing information and data in the corporate repository. As outlined in the *Standard on Email Management*, emails and other messages should not be kept on mobile devices or in email accounts, as these locations do not meet the requirements for sharing, using, safeguarding and storing information and data of business value.
- When creating or collecting information and data of business value, ensure that metadata for key profile fields is maintained.
- Ensure that datasets or information that are evergreen or require regular updating to maintain relevance are updated at appropriate intervals using a designated resource.
- Respect information and data security and privacy requirements when creating or collecting information and data. Refer to subsection 3.6 and subsection 4.6 of this guideline for more information on specific considerations for privacy and security. Specifically, in relation to security, also consult the Mandatory Procedures for Information Management Security Control.
- Respect official languages policies and guidelines when creating or collecting information and data.

2. Information and data management

Organize information and data systematically so that they are easy to discover, access, share and reuse, as permitted within the current legislative and policy environment. Where possible, use standards, rules, tools and procedures put in place at the enterprise level or established by your organization. This practice involves:

- Ensuring that information and data assets are inventoried on a regular basis. This inventory should cover what information and data you have, where they are located, how they are stored, who stewards and has access to them, whether they are shared (outside the organization, beyond borders or jurisdictions), and any privacy and security considerations associated with them.
- Ensuring that information and data are aligned with departmental architecture taxonomies and classifications, as appropriate.
- Ensuring the privacy of information and data and guarding against unauthorized collection, access, disclosure or destruction.
- Where relevant (for example, in cases involving sharing data between government organizations or preparing data for release or publication), ensuring that information and data are aligned with enterprise-level common architecture taxonomies and classifications. For example, if planning on sharing a dataset with information on provinces and territories, it is important to ensure that the values used to express this information align with the relevant reference data standards at the enterprise level. The same applies to data domains for which authoritative sources (for example, master data) at the enterprise level can be found.
- Clearly defining roles, responsibilities and accountabilities for information and data in the organization, both at the working and senior levels. These can be situated as part of a broader departmental governance structure that ensures that issues related to information and data are horizontally tabled and addressed.
- Ensuring that security, privacy and other legal risks are considered in order to improve readiness to release information and data on the open government portal.

Protecting information and data involves preserving their integrity and authenticity. Such protection includes:

- Storing all information and data in a manner that preserves their fitness for purpose and keeps their structure, context, and content intact.
    - An information or data asset's **structure** (format and links to other documents or attachments), its **context** (information about the sender, recipient(s), and the date and place of creation), and its **content** (the text, data, symbols, numerals, images, sound, graphics and other information that make up the substance of the record) are key

elements that preserve the value of the data or information in any medium, provided the elements remain intact.

- Protecting information and data against loss, damage, unauthorized access, alteration, disclosure or destruction. Such protection includes informing contractors of their responsibility to protect any information and data that has been entrusted to them, as well as their responsibilities to provide records should they be requested through an access to information request.
- Marking any information and data according to their appropriate security classification(s), using the relevant metadata field in the electronic document profile (or adding a visible marking to the paper document). Avoid applying a classification that is higher or lower than merited by the information and data.
- Adopting a “cloud first” approach to storing information and data categorized at the Protected B level or below, as outlined in subsection 4.3 of this guideline.
- Ensuring that information and data reside within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad (for example, diplomatic or consular mission), as outlined in subsection 4.4 of this guideline.
- Ensuring that security classification structures are able to distinguish information and data labelled as personal information or sensitive data so that they can be properly protected and managed.
- If a privacy breach is suspected, work with your ATIP office to implement your institution’s breach management plans to contain, manage and report on the privacy breach.
- Protecting classified and protected information and data by ensuring that they are securely stored and properly disposed of, as required by established recordkeeping procedures, privacy and security laws and policies, and any other relevant legislation or policy.
- In cases involving paper-based assets, storing classified information and data in approved locked cabinets. Store such assets on open shelves only if the room has been constructed according to the Secure Room “B” standards of the Royal Canadian Mounted Police.
- Avoiding the storage or sharing of any information and data classified above the security level for which your departmental network(s) have been cleared (normally Protected A or B).
- Avoiding the population and combination of fields (or subject lines) that have personal information and data in a way that may compromise the privacy and security of individuals associated with that information and data (or carry risks for the Government of Canada as a whole), in contravention of the requirements of:
  - the *Privacy Act*
  - the *Policy on Privacy Protection* (and supporting instruments)
  - the *Policy on Government Security* (and supporting instruments)
  - other relevant legislation or policy

- Implementing effective, role-based access control procedures to ensure that classified and protected information and data are made available only on a need-to-know basis to those who are authorized to access them. A security clearance does not automatically grant someone the right to see all information and data classified at or below the level of that clearance.

Not all information and data have the same value. Some will need to be kept over the long term to support a department's policy, programming and service needs, or to preserve archival government records that contribute to Canada's documentary heritage. Other information and data can be disposed of when it is deemed to be no longer useful. To this end, the following practices are recommended:

- Regularly assess the value and utility of information and data assets for the following:
  - current departmental needs
  - whether other departments may seek to reuse it in the future
  - external parties that may find value in its release
- Particularly for personal or sensitive information and data, set retention periods according to clearly demonstrated need for legitimate use, which is to be periodically (for example, annually) reviewed and updated accordingly.
- Destroy transitory information and data as soon as they are no longer needed, complying with your department's information management and security procedures. Similarly, a government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information.
- Cooperate with information management and data specialists to properly transfer digital or paper copies of information and data of enduring value to the Government of Canada and Canadians through Library and Archives Canada's regulations and disposition authorizations.

3. Information and data use

In the absence of organizational frameworks, align with existing enterprise and/or international standards on the ethical and secure use of information and data. Developing or adopting a framework that addresses issues of data ethics and security can help ensure that information and data are not used (or reused) in ways that create risks or carry adverse consequences for Canadians. The UK Government's Data Ethics Framework provides an example of a best practice in this area. The significance of data ethics is also highlighted in the *Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service*.

Handle sensitive or personal information and data in a way that does not risk identification or re-identification, including through anonymization or pseudonymization practices that allow users to realize the value of data without compromising the privacy of the individuals or entities with whom it may be associated.

Build capacity for evidence-informed decision-making by instituting mechanisms that ensure that fit-for-purpose information and data are used to support each stage of a decision-making process. To maintain transparency, this process needs to be traceable or "auditable" such that the information and data used throughout their various stages can be traced and understood in the context in which they were employed. Evidence-informed decision-making, in conjunction with clear roles and responsibilities for information and data (as required under subsection 4.3.2.3 of the *Policy on Service and Digital*), can also improve accountability.

4. Information and data-sharing

Strive to work in the open by default, subject only to limitations where security, privacy or other legal issues would preclude openness, and steward information and data in a way that enables "tell us once" approaches to service delivery. The Canadian Digital Exchange Platform (CDXP) provides the digital infrastructure needed for effective and interoperable information and data exchange within the Government of Canada. For more information on the CDXP, see subsection 3.3 of this guideline. Decisions to share or exchange data between government departments, including through information-sharing agreements, should be made in compliance with applicable privacy and security policy and legislation, including the Treasury Board *Policy on Privacy Protection* and *Policy on Government Security*. Refer to subsection 3.6 and subsection 4.6 of this guideline for more information on specific considerations related to privacy and security requirements. To minimize vulnerabilities to foreign actors when sharing information and data, it is also important to ensure that all Protected B, Protected C and classified materials are encrypted when in transit outside operations and security zones controlled by the Government of Canada, within Canada or internationally. Refer to the *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)* for more information.

Work to advance the objectives of the *Directive on Open Government* and any relevant Open Government National Action Plan commitments by proactively and purposefully releasing information and data of public value to current and future generations of Canadians. To maximize accessibility and utility, the use of open formats for published information and data is recommended. It is also recommended that non-sensitive information and data be released under an open licence for the public to share and reuse. Decisions to release information and data should be made in compliance with applicable privacy and security policies and legislation, as noted above. Refer to subsection 3.4 of this guideline for more information on specific considerations related to open government.

To maximize their value, information and datasets to be released to the public need to be fit for purpose. To avoid releasing "dead" information and data of little utility to users, assess and control the quality of the information and data deemed appropriate for publication. Existing or emerging enterprise and international data quality standards can be leveraged to achieve this objective. For example, *Statistics Canada's Quality Assurance Framework* is useful for assessing the quality of data. The draft Open Government Data and Information Quality Standards in the Open Government Guidebook is another source of guidance on quality requirements for open data. Interdepartmentally, the Enterprise Data Community of Practice is currently supporting the development of an enterprise-wide standard on data quality.

Any information and data received from external parties, governmental or otherwise, need to be profiled and validated prior to their use or reuse. This practice involves, for example, evaluating the quality of the information and data, and complying with any applicable enterprise-level data standards needed to enable their structural and semantic interoperability.

3.2 Use of digital systems to manage information

3.2.1 Description and associated requirements

The Government of Canada is undergoing a digital transformation. An important part of this transformation includes adopting digital and automated systems to manage departmental information instead of relying on paper-based and manual processes. As the volume of information and data produced by the Government of Canada continues to grow, the need for digital systems that can perform auto-classification and other automated information management processes will increase.

Requirement for departments under the directive
The **departmental CIO, in collaboration with other departmental officials as necessary,** is responsible for: 4.3.1.2 Ensuring digital systems are the preferred means of creating, capturing and managing information.

3.2.2 Why is this important?

Managing information and data efficiently and effectively supports service and program outcomes and helps ensures a modern, service-oriented public service. Digital systems provide systematized support for effective information management and are key to acting in an agile and responsive manner. Services that are supported through digital systems enable seamless, secure, reliable and accessible data available anytime and anywhere, from any device.

Digital systems make it easier to capture, share and manage information and data in a timely and secure manner, and facilitate information search and retrieval. In addition, using digital systems to manage information and data supports more effective collaboration both internally and externally because of the ease with which the information can be shared and tracked.

3.2.3 Considerations in implementing the requirement

Particular attention should be given to the following considerations when creating or choosing a digital information management system:

- Leverage enterprise systems where possible in order to enhance interoperability and realize efficiencies.
- Engage with users before choosing an information management system to ensure that it will meet their needs, as well as business requirements, and conduct ongoing testing with users throughout the process in order to understand how users will interact with the system and to identify glitches and pain points.
- Develop the information management system based on business requirements in an agile manner by taking an iterative approach, running tests end to end with users, and making improvements based on user feedback.

- Consider what security and privacy measures are required in order to appropriately secure and protect the information and data the system will need to manage, and engage with privacy and security officials to ensure that the system complies with all requirements for the collection, sharing and protection of personal information. Refer to subsection 3.6 and subsection 4.6 of this guideline for more information on specific considerations related to privacy and security requirements.
- Consider how the information management system needs to be designed from the outset to ensure that it is accessible and usable for all employees, and ensure that you test accessibility features and all components of the system with a variety of users to make sure it meets the needs of all.
- Map out and analyze existing business processes, and implement automation, auto-classification, machine learning and artificial intelligence, wherever feasible. Refer to subsection 4.5 of this guideline for more information on specific considerations related to automated decision-making.
- Ensure alignment with the GC Business Capability Model to enable government-wide use.

3.3 Enabling interoperability

3.3.1 Description and associated requirements

To deliver services digitally to Canadians, the Government of Canada's systems need to communicate with each other using a common language, vocabulary and standards. They need to interoperate. The two policy and directive requirements under this theme call for deputy heads and departmental CIOs of departments to oversee the management of information and data such that interoperability is enabled to the greatest extent possible while respecting security and privacy requirements. Refer to subsection 3.6 and subsection 4.6 of this guideline for information on specific considerations related to privacy and security requirements.

Requirement for departments under the policy
Deputy heads are responsible for: 4.3.2.4 Ensuring that data are managed to reduce redundancy and enable interoperability.

Requirement for departments under the directive
The **departmental CIO, in collaboration with other departmental officials** as necessary, is responsible for: 4.3.1.3 Ensuring information and data are managed to enable data interoperability, reuse and sharing to the greatest extent possible within and with other departments across the government to avoid duplication and maximize utility, while respecting security and privacy requirements.

These requirements reflect the Government of Canada's acknowledgement of the opportunity that interoperability presents:

- Information and data are invaluable assets for digital government, and they are most valuable when they have the potential to be deployed across different business contexts using interoperable systems.
- Coupled with enterprise-level data standards, an interoperable digital environment enables effective data-sharing and reuse, and consequently reduces redundant data collection practices within and across departments.
- Through an interoperability program, which covers the interoperability of data and systems, the Government of Canada is establishing norms, schemas, standardized tools, agreements, data structures and technologies for machines to exchange information and data effectively in order to reduce redundancy and maximize utility.

- Developing and transforming digital systems to be interoperable requires partnership and collaboration between cross-cutting functional areas of expertise, including enterprise architecture, privacy, data, cyber security, procurement and IT.

3.3.2 Why is this important?

Getting the right information to the right people at the right time, while protecting personal information, is the key to improving digital government services for Canadians. Enabling interoperability across the Government of Canada means making possible the reuse, sharing and management of data in order to avoid duplication and maximize utility across departments.

By enabling interoperability, maximum value can be derived from information and data. Enabling interoperability can:

- improve service experiences for Canadians (for example, enabling a "tell us once" approach)
- spark innovation across government departments, industry and civil society

In addition to ensuring that technical capabilities are in place, it is the responsibility of deputy heads and CIOs to oversee the development and application of a consistent set of rules, agreements, standardized methods and parameters. Interoperability is achieved only when these elements are developed and applied in a modern, secure and consistent way while considering the current legislative environment.

3.3.3 Considerations in implementing the requirements

The following implementation considerations clarify key concepts, describe available tools and make recommendations for deputy heads and departmental CIOs, as they are responsible for managing information and data such that interoperability is enabled. The implementation considerations are guided by the Mandatory Procedures for Enterprise Architecture (Appendix A of the *Directive on Service and Digital*).

Key concepts

- Data reuse: Data reuse refers to deploying information and data assets to business contexts beyond that of their originator. In digital government contexts where reuse follows a set of standards and respects security and privacy requirements, exchanging data between government departments avoids duplication, enhances data quality, and is critical for advancing digital government service experiences for individuals and businesses. If personal information (any information about an identifiable individual) is reused or shared for a purpose (such as a department program or activity) other than that for which it collected, valid consent is required. Refer to subsection 3.6 of this guideline for more information on specific considerations related to privacy.
- Interoperability: Interoperability is a desired characteristic of a digital system wherein interfaces are able to interact to enable information and data deployment beyond the context of their originator.

- Web service: A web service is a standardized, secure and consistent way of sharing a system's functionality and data with other systems. Web services define the parameters for interaction for a set of functionality or data. They stipulate what functionality is provided, what data are accessible, how they are structured and how to interact with it.

How to enable interoperability

In enabling interoperability, departments could consider the following:

- Expose system functionality as web services: The functionality of a system can be reused only when it is exposed (made accessible as web services). As an example, a legacy application that issues approvals or denials requires a web service interface (such as an Application Programming Interface (API) end point) in order to be exposed, through which another application can request approvals. Not exposing that web service would require human intervention and hinder reuse and sharing. Exposing functionality requires making it available from a technical perspective. It does not preclude the requisite controls from a security and privacy standpoint to limit access. Exposing functionality as web services increases the agility of government so that, as citizen expectations and government programs evolve, it is possible to reorganize the interactions between these systems to rapidly and effectively meet those needs. Simply put, exposing system functionality configures the Government of Canada's digital assets as "plug and play" ready while maintaining consistent, secure and controlled access.
- Make web services available through a well-defined interface: APIs provide an efficient, consistent and controlled way to make data accessible to other systems. Using APIs promotes reuse and sharing of data within the Government of Canada and with the Canadian public. Making the Government of Canada's web services and data available through APIs also promotes a digital ecosystem where private industry, civil society, local governments and other external stakeholders can better align their services with those of the federal government.
- Ensure that the data shared with other government organizations or on the open government portal adheres to enterprise data standards: As stated in subsection 4.3.1.1 of the *Policy on Service and Digital*, these standards include, but are not limited to, quality, accessibility, common architecture taxonomies and classifications, and life-cycle management. The Enterprise Data Community of Practice supports the development of data standards in these areas. For more information on how to manage information and data in a way that enables effective sharing and reuse, consult subsection 3.1 of this guideline.
- Publish APIs that have potential for cross-departmental, inter-jurisdictional or public consumption to the Government of Canada API Store.
- Ensure that APIs are designed according to the Mandatory Procedures on Application Programming Interfaces: These mandatory procedures govern how APIs are to be developed across the Government of Canada to better support integrated digital processes across

departments. They describe how to ensure APIs are built resiliently and effectively to enable interoperability across the Government of Canada and where they should be published.

- If personal information is shared within or outside of a department, the development of an information-sharing agreement is to be considered (see *Guidance on Preparing Information Sharing Agreements Involving Personal Information*) in order to ensure that the sharing of personal information complies with applicable privacy legislation and policy. Refer to subsection 3.6 of this guideline for more information on specific considerations related to privacy.
- Make use of the Canadian Digital Exchange Platform (CDXP) where suitable.
- Participate in the Digital Exchange Community of Practice (DXCoP) (accessible only on the Government of Canada network), which is a forum to exchange ideas, provide insights, bring forward challenges, and highlight best practices related to interoperability and data exchange across the Government of Canada.

Tools to enable interoperability

- The Government of Canada API Store is a digital marketplace to find and use reusable APIs. It is a centralized repository where users can find all the Government of Canada's APIs.
- The CDXP helps enable digital government by providing a standard environment to interconnect. The CDXP enables secure, private and real-time information and data-sharing, which allows systems to connect to support citizens and businesses. Departments can make use of the CDXP by first identifying requirements, such as what data or business service (such as address lookups) should be shared, and how the interaction should work (for example, event notification such as a death notice or real-time response required such as verification). The Government of Canada API Store is one tool of the CDXP. The CDXP program of the Office of the Chief Information Officer, TBS, is responsible for defining the use cases and best practices for leveraging CDXP components.

Appendix B: Mandatory Procedures on Application Programming Interfaces of the *Directive on Service and Digital* provides further requirements on how to enable interoperability and build APIs.

3.4 Release of information and data on the open government portal

3.4.1 Description and associated requirement

The two policy requirements under this theme concern the public release of information and data, albeit from different but mutually inclusive perspectives. The first obligates the deputy head of a government department to maximize publication of information and data on the open government portal, and the second obligates that the same deputy head to prioritize disclosure based on public demand.

Consequently, the two requirements must be read together and prompt a proactive approach to information and data stewardship, informed by public engagement. Specific approaches a deputy head may wish to take are outlined below.

Requirement for departments under the policy
Deputy heads are responsible for: 4.3.2.8. Maximizing the release of departmental information and data as an open resource, discoverable through the Government of Canada open government portal designated by the Treasury Board of Canada Secretariat, while respecting information security, privacy, and legal considerations.

This first requirement directs the deputy head of a government department to perform interrelated tasks relating to departmental information and data to make information and data open, while assuming a pre-existing knowledge of the department's information and data holdings. Deputy heads must:

- consider relevant security, privacy and other legal issues relating to their department's information and data holdings, including considerations for information and data as being open by design
- ensure that information and data for publication conform to official languages and accessibility requirements
- maximize the disclosure of information and data not subject to such considerations
- make that information and data discoverable through the open government portal (open.canada.ca)

This responsibility implies a proactive approach to information and data management, with the identification of information and data for release at creation or collection. The requirement applies to all forms of government information and data; prioritization is subsequently expressed in the policy's requirement 4.3.2.9, quoted below.

Deputy heads are responsible for ensuring that the privacy of personal information, as defined in the *Privacy Act* and the *Privacy Regulations*, is protected. Release of personal information without the consent of the individual is a privacy breach.

Requirement for departments under the policy
Deputy heads are responsible for: 4.3.2.9. Prioritizing departmental information and data to be added to the Government of Canada's open government portal, informed by public demand.

This second policy requirement implies that deputy heads of departments perform the following three interrelated tasks relating to public demand for government information and data:

1. consider public demand for the disclosure of government information and data holdings
2. prioritize that information and data for disclosure
3. make that information and data discoverable through the open government portal

Although the policy requirement 4.3.2.8 requires maximizing the disclosure of all government information and data, this requirement explains how to prioritize those disclosures, and thus is mutually inclusive. It implies that deputy heads have an understanding of public demand for their departmental information and data holdings. Specific mechanisms that allow for such an understanding are outlined below.

Taken together, these two policy requirements may be read as follows:

- consider relevant security, privacy and legal obligations relating to the department's information and data holdings
- consider public demand for the disclosure of government information and data
- maximize the disclosure of government information and data on the open government portal in the following order:
    - in accordance with public demand
    - in accordance with all other demands or requirements, including those identified in this policy

3.4.2 Why is this important?

Effective information and data stewardship, meaning a whole-of-life-cycle approach to information and data management, enables many of the hallmarks of a user-centric, evidence-driven and digitally enabled public service. Publishing information and data as open resources is a core feature of effective and client-centric public services and programs, including the promotion of the following:

- greater transparency
- public accountability
- effective governance
- efficient service and program design
- reduced work duplication
- enhanced interdepartmental collaboration on cross-jurisdictional issues
- increased opportunities with non-government stakeholders and service users, including economic and social program innovation

Security, privacy and other legal issues must be addressed at all stages of information and data life-cycle management. To protect privacy, personal information cannot be considered for public release.

3.4.3 Considerations in implementing the requirement

Maximizing the release of information and data on the government portal (requirement 4.3.2.8 of the policy)

The term "maximize" is not defined in the policy, and thus is to be given its dictionary definition, which is to make as large or as great as possible. The scope of possibility for maximizing release is nonetheless subject to prevailing legislation or policy instruments that require that deputy heads also assess security, privacy or other legal risks. In context, this means that information and data should be published as fully and completely as possible on the open government portal, wherever it is determined that there are no privacy, security or other legal risks that prohibit disclosure of information or data. Extensive guidance to supplement the information in this guideline is available through the Open Government Guidebook. Refer to subsection 3.6 and subsection 4.6 of this guideline for more information on specific considerations related to privacy and security requirements.

Notwithstanding the need to conduct risk assessments, it is not sufficient to state that portions of a dataset or other information contain risks and therefore that the whole record cannot be published. Rather, a serious effort is expected to be taken to separate sensitive from non-sensitive information and to publish the remainder. Accordingly, proactive risk mitigation is strongly implied by the term "maximize." Deputy heads are thus encouraged to embrace an "open by design" approach to managing information and data, building in mitigation strategies to the creation of government records and datasets. This approach has the practical benefit of reducing administrative burdens and resource requirements associated with modifying already existing information and datasets.

Importantly, maximizing disclosure of government information and data is not a one-time activity. Many datasets and other sources of government information require regular updating. Deputy heads are encouraged to develop schedules for updating relevant information and data sources.

To the extent possible, and wherever relevant, it is recommended that deputy heads also ensure that government officials responsible for collecting data or creating datasets do so in a manner that is disaggregated by the lowest possible administrative categories. The eligibility for release of disaggregated data is subject to privacy and other legal obligations. Refer to subsection 3.6 of this guideline for further details on privacy requirements. Depending on the circumstances, maximizing disclosure of information and data also means maximizing the full breadth of the data, rather than in an aggregated form, to ensure that evidence used in creating policies and programs is appropriate and that there are no gaps are present. This consideration would need to be identified at creation or collection, and would support other government priorities of inclusion and client-centric design.

Prioritizing information and data to be added to the government portal (requirement 4.3.2.9 of the policy)

Deputy heads retain some flexibility in how they assess public demand for information or data. These methods may include, but are not limited to the following:

- conducting client or user surveys
- analyzing frequent or repeat requests made under the *Access to Information Act*
- consulting and engaging with relevant stakeholder groups or communities, in keeping with public engagement principles
- reviewing requests received through interactions with the public or stakeholders, including on social media and through communication centres
- reviewing requests received during events, including conferences, presentations, workshops with educational institutions, and hackathons
- identifying issues or priorities of the government or department (for example, climate change, environmental issues, explanations) of programs
- responding to requests received through the "suggest a dataset" feature on the open government portal

For the last of these, deputy heads are encouraged to ensure that a designated official within their organization receives and is responsible for responding to dataset suggestions originating from the open government portal.

Prioritizing, although informed by public demand, may nonetheless be subject to other considerations (for example, core mandate datasets disclosed as part of the Management Accountability Framework). The policy does not define this process, although it should be understood as a discretionary exercise. As above, regarding privacy or security considerations, it is insufficient to favour one priority over another without undertaking a significant weighing exercise. Factors to consider may include but are not limited to the following:

- the type and frequency of public demand

- feasibility of disclosure
- timeliness issues
- potential impact of disclosure
- the existence of other more appropriate mechanisms to obtain information (for example, other legislated obligations)

Where it is deemed that public demand can be met, data or information requested by the public should be published on the open government portal by employing the same considerations as for requirement 4.3.2.8.

Lastly, publication of information on the open government portal must adhere to the requirements in the *Open Government Guidebook*.

3.5 Accessibility by design

3.5.1 Description and associated requirements

This theme is about making digital information, as well as information, communication and technology (ICT) solutions and equipment, accessible at the outset (that is, when they are designed or created). Accessible digital information and ICT solutions and equipment mean that they are fully usable by all, that is, by persons with and without disabilities. Accessibility allows clients and users to navigate through the information or use solutions and equipment in different ways.

In addition to being a cross-cutting consideration to keep in mind when implementing a number of requirements of the *Policy on Service and Digital* and the *Directive on Service and Digital*, accessibility is specifically mandated in the following requirements.

Requirement for TBS under the policy
The **CIO of Canada** is responsible for: 4.4.1.3 Providing direction and defining enterprise-wide requirements for Information and Communication Technologies (ICT) accessibility.

The CIO of Canada has a role to play in providing direction to departments as it relates to accessible ICT.

Requirement for departments under the policy
Deputy heads are responsible for: 4.4.2.2 Ensuring that, for newly procured or developed information, communication, and technology solutions and equipment, applicable requirements or standards regarding accessibility […] are addressed by design.

This policy requirement means that accessibility should be considered early in the process of procuring or developing new ICT solutions and equipment, that is, at the design stage. This requirement also includes considerations other than accessibility, which are explained in subsection 4.1 of this guideline.

Requirement for departments under the directive
The **departmental CIO**, in collaboration with other departmental officials as necessary, is responsible for: 4.3.1.4 Ensuring departmental information is created in an accessible format, where appropriate, in accordance with TBS guidance.

This directive requirement is about the production and availability of accessible and usable digital information, which includes embedded content (for example, hyperlinks to other sources of information). Accessible digital information includes both web and non-web information. Non-web documents may include letters, emails, books, spreadsheets, presentations and videos that have associated user agents such as a document reader, editor or media player.

3.5.2 Why is this important?

Proactive consideration of accessibility benefits everyone in Canada, especially persons with disabilities. Accessible digital information and ICT solutions and equipment:

- assist everyone
- facilitate the inclusion of a diverse segment of Canadians
- enable a significant segment of the population with diverse functional needs and abilities to participate fully and productively in all aspects of life, including effective interaction with the Government of Canada, as citizens, service clients and public servants

Accessibility is also grounded in a number of foundational statutes, including:

- the Canadian Charter of Rights and Freedoms, which enshrines the equality of persons with disabilities
- the *Canadian Human Rights Act*, which includes disability in the prohibited grounds of discrimination
- the *Accessible Canada Act*, which includes requirements for federal departments to identify, remove and prevent accessibility barriers, including in the area of ICT

3.5.3 Considerations in implementing the requirements

Accessible ICT solutions and equipment

Policy requirement 4.4.2.2 applies to newly procured and developed Government of Canada ICT solutions and equipment, whether they are internal or public-facing, including IT tools and equipment for federal public servants.

Refer to the *Guideline on Making Information Technology Accessible by All* for implementation considerations when procuring or developing new ICT solutions and equipment that are accessible. The guideline also proposes additional considerations to improve accessibility as part of the life-cycle management of existing ICT solutions and equipment, including digital information.

Accessible digital information

The production of accessible digital information can be effectively accomplished by ensuring that information is perceivable, operable, understandable and robust to respond to the needs, abilities, work and interface techniques of a diverse group of users, as outlined in the following.

Perceivable

- Provide text alternatives for non-text content
- Provide captions and other alternatives for multimedia

Operable

- Users of various tools must be able to read, navigate and edit digital information with ease. For example:

  - make all functionality available from a keyboard
  - give users enough time to read and use content
  - do not use content that causes seizures or physical reactions (for example, rapidly flashing images)
  - help users navigate and find content
  - make it easier to use inputs other than by using a keyboard

Understandable

- Create content that can be presented in different ways, including through assistive technologies without losing meaning

Robust

- Ensure that users can access and interact with digital content by relying on various hardware and software products and configurations

The overarching objective of these principles is to better respond to the needs of a diverse set of users. For example, a blind user may use a screen reader or a braille display. A person who has a motor impairment may use a keyboard rather than a mouse. Other users may need to adjust font size or spacing to compensate for vision loss or cognitive disabilities.

Refer to the Treasury Board *Standard on Web Accessibility* for requirements applicable to public-facing web content.

Collaborative approach

Digital content production methods evolve rapidly as technology advances. Therefore, achieving consistent accessibility across departments requires a collaborative approach.

Although TBS provides guidance on digital accessible information and ensures the availability of up-to-date training, including through courses delivered by the Canada School of Public Service, departments are encouraged, through internal activities, to ensure that:

- all employees are aware of the importance of accessibility and associated legal and policy requirements
- employees receive regular training and updates on fundamental and emerging accessibility techniques and methods
- practical resources are available to all employees

Practical resources and other references

- The Treasury Board and the Public Service Commission of Canada *Policy on the Duty to Accommodate Persons with Disabilities in the Federal Public Service* establishes requirements for departments to create and maintain an inclusive, barrier-free environment in the federal public service to ensure the full participation of persons with disabilities.
- Additional requirements pertaining to accessibility can be found in:
  - *Policy on the Planning and Management of Investments*
  - *Policy on Communication and Federal Identity*

- The Government of Canada's *Accessibility Strategy for the Public Service of Canada* commits to high standards for accessibility in its policies, programs and services to all Canadians.
- Shared Services Canada's *Accessibility, Accommodation, and Adaptive Computer Technology Program (AAACT)* has a collection of guides (accessible only on the Government of Canada network) that provide practical assistance in creating accessible and usable digital information

Resources from other jurisdictions include the following:

- Ontario Government Accessible Digital Office Document Project
- IBM Accessibility Research (including checklists and guides)
- Microsoft Accessibility Overview
- GOV.UK Accessibility and assisted digital
- Queen's University Accessibility Hub
- Web Content Accessibility Guidelines (WCAG) Overview
- United Nations Convention on the Rights of Persons with Disabilities

3.6 Privacy and protection of personal information

3.6.1 Description and associated requirements

The policy requirements in this section ensure that the privacy and security of personal information held by departments is protected in all activities governed by the *Policy on Service and Digital* and the *Directive on Service and Digital*.

More detailed guidance on privacy protection can be found in the policies and directives issued in support of the administration of the *Privacy Act*.

Requirements for departments under the policy

Deputy heads are responsible for:

4.3.2.5. Ensuring that, when managing personal information or data, including in the context of data interoperability, the privacy of individuals is protected according to the *Privacy Act* and any other relevant legislation, policy or agreement.

4.3.2.6. Ensuring that privacy is addressed in the context of any plan or strategy to manage departmental information or data.

4.3.2.7. Ensuring that sensitive information under the department's control is protected according to the *Policy on Government Security* and any relevant legislation, policy or agreement.

These three policy requirements direct deputy heads of government departments to establish sound privacy practices to protect and manage personal information under their respective department's control, consistent with the requirements of the following:

- *Privacy Act* and *Privacy Regulations*
- *Policy on Privacy Protection*
- *Directive on Privacy Practices*
- *Directive on Privacy Impact Assessment*
- *Directive on Personal Information Requests and Correction of Personal Information*

Deputy heads are also required to ensure that the requirements of the *Policy on Government Security* for the protection of sensitive information are met.

Key requirements for the protection of privacy include the following:

- ensuring that privacy practices are consistent with and respect the provisions found in the *Privacy Act,* the *Privacy Regulations* and other applicable legislation, including the institution's enabling legislation

- ensuring, before collecting personal information, that the institution has parliamentary authority for the program or activity for which the information is being collected and that the institution is collecting only the personal information that is needed
- ensuring that a Privacy Impact Assessment for a program or activity is conducted for new or substantially modified programs or activities when personal information is used or intended to be used
- ensuring that personal information is as accurate, up-to-date and complete as possible
- limiting access to, and use of, personal information by administrative, technical and physical means in order to protect that information
- establishing plans and procedures for addressing privacy breaches
- applying the institution's standards for the retention of personal information, as well as the disposition standards as established by Library and Archives Canada

Requirement for departments under the directive
The **departmental CIO, in collaboration with other departmental officials** as necessary, is responsible for: 4.3.1.9 Protecting information and data by documenting and mitigating risks, and by taking into consideration the business value of the information, legal and regulatory risks, access to information, security of information, and the protection of personal information.

This directive requirement ensures that departmental CIOs (and other departmental officials) protect personal information and data under their control by documenting and mitigating risks. To fulfill this requirement, departmental CIOs must:

- in collaboration with other departmental officials, establish practices for protecting and managing personal information to fulfill the requirements of the *Directive on Privacy Practices* regarding departmental activities that involve the creation, collection, retention, accuracy, use, disclosure or disposition of personal information under the department's control
- if a privacy breach is suspected, work with your ATIP office to implement your institution's breach management plans to contain, manage and report on the privacy breach
- identify, document, and mitigate privacy and security risks in accordance with the *Directive on Privacy Impact Assessment*

3.6.2 Why is this important?

The protection of privacy is an essential element in maintaining public trust. It is a core responsibility of government and is integral to managing information held by government institutions. Canadians expect government departments to respect the spirit and requirements of the *Privacy Act*, the *Privacy Regulations* and associated policies to safeguard their privacy in a modern, data-driven environment.

These requirements aim to ensure that government departments collect, use, retain and disclose personal information in accordance with the requirements of the *Privacy Act*, the *Privacy Regulations*, and associated policies and directives.

3.6.3 Considerations in implementing the requirement

Under the *Privacy Act*, personal information refers to any information about “an identifiable individual that is recorded in any form.” Such information includes, for example, an individual’s address, Internet Protocol address(es), employment or medical history, personal opinions, and identifying numbers such as social insurance numbers. Some personal information (for example, health information, government-issued pieces of identification) is more sensitive than others. Generally, the more sensitive the information, the higher the risk of harm to individuals, and therefore the greater the requirements associated with ensuring its security.

Personal information must be collected, retained, used, disclosed and disposed of only in a manner that respects the provisions of the following:

- *Privacy Act* and *Privacy Regulations*
- *Policy on Privacy Protection*
- *Directive on Privacy Practices*
- *Directive on Privacy Impact Assessment*
- *Directive on Personal Information Requests and Correction of Personal Information*

Your institution’s ATIP office can advise you on these requirements.

Security considerations

The *Policy on Government Security* provides direction on security controls in support of the trusted delivery of programs and services, including the protection of personal information under the Government of Canada’s control.

Mandatory Procedures for Enterprise Architecture Assessment (Appendix A of the *Directive on Service and Digital*) stipulates specific procedures to be followed as they relate to business architecture, information architecture, security architecture and privacy. The Standard on Security Categorization (Appendix J of the *Directive on Security Management*) provides details on security categories that must be applied to different types of information.

Departments should also consult the Standard on Security Event Reporting and the *Government of Canada Cyber Security Event Management Plan*.

For more information on managing cyber security events, refer to subsection 4.6 of this guideline.

4. Leveraging technology

Canadians are living in an era where rapid technological changes are altering the way they live, work and interact with each other. They expect their government to adapt how it operates, designs and provides services to meet their needs. Technology provides an opportunity for government to better understand its citizens, improve its services to meet their needs, and operate more efficiently.

In order to leverage the opportunities that technology offers, sound management is key. This section provides information on requirements related to managing technology. It outlines a balanced approach by explaining how departments can make use of new methods, tools and technologies, while ensuring that important considerations related to ethics, accessibility, protection of personal information, security and other aspects are addressed at the outset.

Among the expected outcomes of the *Policy on Service and Digital* is that technology is leveraged to enable business and program innovation and service delivery.

4.1 Considerations at the design stage

4.1.1 Description and associated requirement

This requirement requires deputy heads to ensure that accessibility, official languages, protection of personal information, the environment, and security requirements or standards are addressed **by design** when procuring or developing information, communication and technology (ICT) solutions and equipment.

Requirement for departments under the policy
Deputy heads are responsible for: 4.4.2.2 Ensuring that, for newly procured or developed information, communication, and technology solutions and equipment, applicable requirements or standards regarding accessibility, official languages, protection of personal information, the environment, and security are addressed by design.

4.1.2 Why is this important?

It is important to address requirements or standards for the following to ensure that users and clients have access to solutions and equipment that they can safely use, no matter their ability or official language spoken:

- accessibility
- official languages
- protection of personal information
- the environment

- security in the design of procured or developed ICT
- contracting and other arrangements

Although various requirements already exist, this requirement of the policy underscores the importance of addressing all of these considerations **at the design stage of ICT procurement or development**. There are clear benefits related to this approach, including:

- better anticipation of root causes of issues, increasing the ability to remediate at the source
- increased awareness of issues and risks at an early stage
- simpler and less costly solutions by identifying potential problems at the outset and decreasing the need for retrofitting at a later stage
- better ICT solutions and equipment for users and clients of all abilities and needs, promoting confidence in government and contributing to better experiences for users and clients
- avoided major failures related to ICT procurement and development experienced by the Government of Canada and other jurisdictions
- avoided breaches of relevant laws and administrative policies
- minimized negative environmental impacts and considered greenhouse gas emissions of ICT procurement and development

4.1.3 Considerations in implementing the requirement

Before spending valuable and limited resources on designing, an essential step is to articulate the problem, identify the root cause, and communicate the desired business outcomes. Doing so allows stakeholders to understand why the problem is important, how it came to be, and what is expected to happen once the problem is resolved. This analysis:

- creates the foundation on which all other work is built
- provides a consistent understanding among stakeholders
- sets a clear direction for stakeholders to work toward

These aspects can be articulated using a concept case that was introduced in April 2018. Mandatory Procedures for Concept Cases for Digital Projects (Appendix C of the *Policy on the Planning and Management of Investments*) describes when a concept case is necessary and provides a template to be used. Even if a project does not meet the criteria to submit a concept case, this template can still be used, as this information is important for any initiative.

Considerations at the design stage

Mandatory Procedures for Enterprise Architecture Assessment outlines the assessment framework to be used by departmental enterprise architecture review boards and the Government of Canada Enterprise Architecture Review Board to review digital initiatives, which includes procured and developed ICT solutions and equipment. These mandatory procedures guide departments in assessing their procurements and in developing ICT solutions and equipment. In addition to the requirements in these mandatory procedures, the following requirements and standards should be considered **in the design** of ICT solutions and equipment:

Accessibility

Refer to subsection 3.5 of this guideline for information on specific considerations related to newly procured or developed ICT solutions and equipment.

Official languages

When procuring or developing ICT solutions and equipment, the following should be taken into consideration at the design stage:

- *Official Languages Act*
- *Policy on Official Languages*

Protection of personal information

When procuring or developing ICT solutions and equipment, the following should be taken into consideration at the design stage:

- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act (Part 2)*
- *Policy on Privacy Protection*

Refer to subsection 3.6 of this guideline for information on specific considerations related to privacy and protection.

Environment

When procuring or developing ICT solutions and equipment, the following should be taken into consideration at the design stage:

- *Policy on Green Procurement*

Security

When procuring or developing ICT solutions and equipment, the following should be taken into consideration at the design stage:

- *Security of Information Act*
- *Policy on Government Security*
- *Directive on Security Management*
  - Appendix B: Mandatory Procedures for Information Technology Security Control
  - Appendix J: Standard of Security Categorization
- *Standard on Security Screening*
- *Directive on Service and Digital*
  - Appendix A: Mandatory Procedures for Enterprise Architecture

Refer to subsection 4.6 of this guideline for information on specific considerations related to cyber security.

The above considerations are also key elements of providing client-centric services, which is discussed in detail in subsection 2.1 of this guideline.

4.2 Digitally enabled operations

4.2.1 Description and associated requirement

The *Policy on Service and Digital* defines digitally enabled operations as operations that are supported by strategically leveraging information and communications technologies, infrastructures, and the information and data they produce and collect. Simply put, this means that the government takes advantage of modern, digital means to operate and deliver services to Canadians. Doing so includes operating in a digital-first and integrated environment and supporting workers with digital tools to facilitate efficiency and effectively deliver on the goals of the Government of Canada.

Requirement for directed at departments under the policy
Deputy heads are responsible for: 4.4.2.1. Ensuring departmental operations are digitally enabled.

4.2.2 Why is this important?

Adapting government to leverage new technologies and ways of working is one of the major digital challenges, and an opportunity, that government faces in the coming years. The shift to digitally enabled government operations has the potential to transform the way Canadians interact with and access services from the government. A digitally enabled government can be more responsive to emerging issues and user needs, and be more agile in its approach to decision-making and service delivery.

An organization that is digitally enabled can be more efficient, effective and responsive. This is because digital tools have the potential to simplify and speed up cumbersome analogue processes such as paper-based applications for services. Furthermore, digitally enabled operations support an open and collaborative government and public service by providing fast, secure platforms for information and data exchange and collaboration.

4.2.3 Considerations in implementing the requirement

A government that has digitally enabled operations allows public servants to access integrated information and data systems, which in turn provides consistency, exposes gaps and duplications, enables richer analysis, and supports multi-channel service delivery.

A digital government builds digital delivery methods into its operations and service design, and provides the required tools to digitally enable interactions across the public service, through all windows and service channels, including traditional avenues such as over the telephone or in person.

See subsection 2.3 of this guideline for more information on online services.

How to digitally enable operations

Following are some implementation considerations that could help ensure that departmental operations are digitally enabled:

- Review existing internal and external business processes and identify those that could benefit from the use of digital tools and processes (for example, applications for government services, licences, permits, approval processes). Consider how traditionally analogue processes can be supplemented with digital mechanisms (for example, using voice-to-text technology to offer a more inclusive experience for persons with disabilities by providing real-time text closed captioning).
- Consider how digital tools and processes can be used to improve service delivery and client satisfaction, for example, by simplifying client access to Government of Canada services (such as a single account or where the user only has to "tell us once") or leveraging artificial intelligence technology and analytics to gain insights into the customer experience.
- Consider how back-end operations can be digitally optimized and made more efficient (for example, through the use of workflows, automatic classification, artificial intelligence, machine learning).
- Integrate core business applications so that systems can share information and data and reduce duplication of efforts and resources (for example, financial application systems integrated with a Electronic Document and Records Management Solution (EDRMS)).
- Provide a modern workplace fit-up, such as tablets or laptops, mobile computing, extended Wi-Fi capabilities, web conferencing and support for telework arrangements. A fit-up is an excellent opportunity to drive forward the digital principles of using the right tools for the job, being inclusive and providing support for those who need it. Refreshed and open work environments and tools, which promote local and interdepartmental collaboration, may contribute to employees feeling respected and supported, and to better outcomes.
- Where possible, consider making systems and processes open by design to enable collaboration, interoperability and improved user experience.
- Ensure consistency and interoperability across all delivery channels, including in person, telephone and online.
- Implement considerations (for example, security, privacy, accessibility) at the design stage according to subsection 4.1 of this guideline so as to continually maintain and operate services and programs and reduce likelihood of system failures.

- Include continual improvement processes as part of your evaluation approach to ensure that systems (such as operational systems and business applications) are kept updated and modern.
- Where relevant, leverage a cloud-first approach, as outlined in subsection 4.3 of this guideline.
- Regularly review and update all operational business requirements to ensure that needs are current and met (for example, operating a service-oriented department that considers workers' evolving needs, and keeping departmental systems up-to-date to ensure security).
- Design processes to ensure that workers have the digital tools and training required to operate in a modern and responsive environment (for example, establishing and executing a plan for regularly replacing and upgrading hardware, providing learning opportunities and training supports to personnel, and conducting regular surveys with users to find out what digital tools they need).
- Engage in cross-departmental collaboration and sharing for choosing and analyzing the best use of emerging, modern and updated digital tools and services (for example, the GCdocs Information Management Directors' Steering Committee helps prioritize new functionality to be provided by the Public Services and Procurement Canada GCdocs program and shares best practices and lessons learned for EDRMS adoption within departments).
- Link these activities to departmental governance and decision-making processes. See subsection 1.1 of this guideline for more information.

4.3 Cloud services

4.3.1 Description and associated requirements

Public cloud computing can be compared with public utilities that deliver commodities such as electricity. Instead of buying and running infrastructure itself, an organization buys computing power from a provider. In a public cloud model, vendors are responsible for maintaining and renewing the infrastructure, upgrading applications and adding new capabilities, and customers purchase computing power on demand rather than acquiring and operating the infrastructure themselves.

Requirements for departments under the directive

The **departmental CIO** is responsible for:

4.1.1.2 Submitting to the Government of Canada enterprise architecture review board proposals concerned with the design, development, installation and implementation of digital initiatives:

- 4.1.1.2.4 That are categorized at the protected B level or below using a deployment model other than public cloud for application hosting (including infrastructure), application deployment, or application development;

4.4.1.9 Supporting the use of cloud services first by ensuring they are:

- 4.4.1.9.1 Identified and evaluated as a principal delivery option when initiating new departmental, enterprise, and community of interest cluster IT investments, initiatives, strategies and projects;
- 4.4.1.9.2 Adopted when they are the most effective option to meet business needs; and
- 4.4.1.9.3 Compliant with appropriate federal privacy and security legislation, policies and standards.

Requirements for departments under the directive

4.1.1.2 Submitting to the Government of Canada enterprise architecture review board proposals concerned with the design, development, installation and implementation of digital initiatives:

- 4.1.1.2.4 That are categorized at the protected B level or below using a deployment model other than public cloud for application hosting (including infrastructure), application deployment, or application development;

4.4.1.9 Supporting the use of cloud services first by ensuring they are:

- 4.4.1.9.1 Identified and evaluated as a principal delivery option when initiating new departmental, enterprise, and community of interest cluster IT investments, initiatives, strategies and projects;
- 4.4.1.9.2 Adopted when they are the most effective option to meet business needs; and
- 4.4.1.9.3 Compliant with appropriate federal privacy and security legislation, policies and standards.

The *Directive on Service and Digital* calls for a "cloud-first" approach, that is, that public cloud is to be considered as the primary model for systems and data that are categorized at the Protected B level or below.

Cloud is applicable to new investments and for addressing end-of-life technologies and data centre closures.

When proposals at the Protected B categorization level or below are undertaken that do not use a public cloud deployment model, they must be submitted to the GC Enterprise Architecture Review Board (GC EARB) for assessment. See subsection 1.4 of this guideline for information on when and how to submit initiatives to GC EARB. Although public cloud may not always be the optimal deployment model for technology, the GC EARB would like to review and assess such proposals.

4.3.2 Why is this important?

Cloud is shifting the way IT is being delivered. Cloud allows for the improvement of the stability and security of existing systems and services and better balances supply and demand. It also enables universal access to shared systems and higher-level services, all of which can be rapidly deployed with minimal effort, leading to improved coherence and economies of scale.

Cloud services are important because Canadians increasingly expect the government to:

- deliver digital services that give them the same quality of user experience they get from commercial service providers, such as financial institutions, online shopping services and social media services
- deliver digital services with the agility and speed necessary to keep pace with changing legislation and government service offerings
- minimize the IT life-cycle management costs of applications and infrastructure

4.3.3 Considerations in implementing the requirements

The table below provides a summary of the cloud deployment models available to departments and suggests when the usage of each might be appropriate.

Application strategy	**Innovate or migrate**	**Migrate or tolerate**	**Tolerate**
Deployment model	**Public cloud** is an existing commercial multi-tenant offering. Public cloud is the default deployment model for applications at or below the Protected B level. Public cloud is used when deploying new applications or when modernizing applications to address technical or business risks, including migration from legacy data centres.	**Enterprise data centres** are existing modern data centre facilities that are appropriate when an existing application must be migrated due to decommissioning of an at-risk legacy data centre, but the cost of refactoring or replacement required to migrate the application to a cloud environment is extremely high (that is, tens of millions of dollars for a single application). This model is not acceptable for new applications unless the data is categorized above Protected B.	**Legacy data centres** are data centre facilities that existed prior to the availability of enterprise data centres. Legacy data centres are the point of origin for application migration. They are no longer a target for application migration.

The *Government of Canada Cloud Adoption Strategy* describes the government strategy for adopting cloud services and provides background information, definitions and key implementation considerations.

As directed by requirement 4.1.1.2.4 of the *Directive on Service and Digital*, proposals of digital initiatives that are categorized at the Protected B level or below and that are using other system development and delivery options must be submitted to the GC EARB before proceeding, using the GC EARB Presenter Template on the GC EARB GCcollab page. See subsection 1.4 of this guideline for information on when and how to submit initiatives to the GC EARB.

Cloud services must be used in compliance with the requirements of the *Policy on Government Security* and the *Directive on Security Management*. The *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)* supports departments in understanding the Treasury Board's security policy requirements in the context of cloud computing and provides guidance to assist in the secure use of commercial cloud services. Additionally, tools and templates are available to help secure cloud environments:

- Government of Canada Enterprise Security Architecture (GC ESA) Artifact Repository
- Government of Canada ESA Cloud Security Initiative
- Canadian Centre for Cyber Security – Publications (filter topics by "cloud security")

Cloud services must also be used in compliance with privacy-related laws and policies. Refer to subsection 3.6 of this guideline for information on privacy and protection.

Finally, the Government of Canada provides a consolidated cloud services landing page for all public-facing cloud documentation, including strategy, risk assessments and interpretation of existing policies in the context of cloud.

4.4 Data residency

4.4.1 Description and associated requirement

Data residency refers to the physical or geographic location of an organization's data while at rest. This is distinct from data sovereignty, which refers to a country's right to control access to and disclosure of digital information that is subject to its own legislation. For more information on data sovereignty, refer to Government of Canada White Paper: Data Sovereignty and Public Cloud.

Requirement for departments under the directive
The **CIO** is responsible for: 4.4.1.10 Ensuring computing facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic or consular mission, be identified and evaluated as a principal delivery option for all sensitive electronic information and data under government control that has been categorized as Protected B, Protected C or is Classified.

A Government of Canada–approved computing facility is one that is located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic or consular mission. For clarity, the computing facility does not need to be owned by a Canadian corporation, as this could be in violation of trade agreements of which Canada is a party.

Classified electronic data (that is, classified as Confidential, Secret or Top Secret) is data that if compromised would reasonably be expected to cause an injury to the national interest. Such data includes all data that falls within the exemption or exclusion criteria under the *Access to Information Act* and the *Privacy Act*. Data described in the exclusion criteria is deemed to be important either to preserving the national interest or to protecting other interests for which the government assumes an obligation. Classified data also includes data that has regulatory or statutory prohibitions and controls. Protected B and Protected C electronic data is data that, if compromised, could cause serious or extremely grave injury to an individual, organization or government. Consult the Levels of security tool and the Standard on Security Categorization for more information on levels of security and information confidentiality categories.

4.4.2 Why is this important?

Data residency is important because it can impact Canadians' confidence in government decisions. The public may perceive the storing of their sensitive data outside of Canada's borders to be at risk. Data residency is also an important issue that departments face as they increasingly move information to the cloud.

There is a growing need to ensure that data is protected and complies with data residency, privacy and security requirements. For clarity, this requirement applies to all electronic data whether hosted in a cloud environment or not.

4.4.3 Considerations in implementing the requirement

Whether the data resides in Canada or outside, departments must continue to apply appropriate controls, in accordance with the Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice and the *Directive on Security Management*. Controls include ensuring that all Protected B, Protected C and classified Government of Canada electronic data is encrypted when in transit.

Before using cloud services to support departmental programs and services, departments are expected to identify and categorize information based on the degree of injury that could be expected to result from a compromise of its confidentiality, integrity and availability. For more information, refer to subsection 4.3 and subsection 4.6 of this guideline.

The departmental CIO is responsible for approving departmental decisions to store data outside Canada. However, in the case where a department provides enterprise-wide services, it is recommended that the CIO of Canada approve decisions related to data residency.

The following criteria are to be considered when evaluating the option to store data outside Canada:

- Reputation: It is important that Canadians continue to trust the Government of Canada and the decisions it makes. Evaluation to move data outside Canada is to consider how the average Canadian, media or critic of the government would perceive the Government of Canada's decision to store the dataset outside Canada.
- Legal and contractual considerations: Subject to any agreements, laws or policies that Canada has made to the contrary, Canada is generally not restricted to keeping data in Canada. More information can be found in the following:
  - Guidance Document: Taking Privacy into Account Before Making Contracting Decisions
  - Government of Canada White Paper: Data Sovereignty and Public Cloud
- Trade agreements: Procurements must comply with Canada's obligations under its trade agreements not to discriminate against suppliers that store data outside Canada. Some of those trade agreements allow the Government of Canada to restrict sensitive data to Canada where data residency is a legitimate operational requirement or for other reasons. However, any such restrictions must be imposed in accordance with the requirements of the trade agreements.
- Market availability: If the required capabilities allow data to remain isolated to Canada, those capabilities should be considered first. However, some solutions cannot isolate data to Canada

or may not yet be able to isolate data to Canada. It is important to understand how the provider will evolve the capabilities of the desired service.

- Business value: The evaluation should weigh how any business value gained against any perceived risks of moving the data outside of Canada.
- Technical capabilities: Consider whether there are sufficient technical capabilities available that would provide Canadians with additional assurance that data moved outside of Canada will remain protected.

The following table provides a summary of data residency restrictions.

Categorization level	Data residency
Unclassified	No policy restrictions
Protected A	No policy restrictions
Protected B	Facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad are identified and evaluated as a principal delivery option.
Protected C	Facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad are identified and evaluated as a principal delivery option.
Classified (Top Secret, Secret or Confidential)	Facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad are identified and evaluated as a principal delivery option.

4.5 Automated decision-making

4.5.1 Description and associated requirements

Automated decision-making is when technology is used to produce assessments about a particular individual or case meant either to directly aid a human in their decision-making or make a decision in lieu of a human.

The *Policy on Service and Digital* states that deputy heads are responsible for ensuring the responsible and ethical use of automated decision-making systems. The supporting *Directive on Automated Decision-Making* aims to ensure that automated decision-making systems are used in a manner that is compatible with core administrative law principles, such as transparency, accountability, legality and procedural fairness. This directive also includes an Algorithmic Impact Assessment (AIA) tool designed to help departments assess and mitigate risks associated with deploying an automated decision-making system. The AIA also helps identify the impact level of automated decision-making systems.

Requirements for departments under the policy
Deputy heads are responsible for: 4.4.2.4 Ensuring the responsible and ethical use of automated decision systems, in accordance with TBS direction and guidance, including: 4.4.2.4.1 Ensuring decisions produced using these systems are efficient, accountable, and unbiased; and, 4.4.2.4.2 Ensuring transparency and disclosure regarding use of the systems and ongoing assessment and management of risks.

4.5.2 Why is this important?

This policy requirement and supporting directive requirements aim to reduce risks to Canadians and federal departments when using automated decision-making systems and ensure efficient, accurate, consistent and interpretable decisions, which are made pursuant to Canadian law. Early action from departments is being proposed in their adoption of automated decision-making systems so that they can address implementation concerns of bias and lack of transparency at the outset. This proactive, consistent and responsible approach also minimizes the Government of Canada's legal liability and public-facing risks.

4.5.3 Considerations in implementing the requirements

The implementation considerations below are guided by the *Directive on Automated Decision-Making* (the directive).

Initiation phase

Complete the AIA early in the initiation phase, as the results of the AIA (specifically the "impact level") will articulate the mitigation and/or consultation requirements to be addressed in the implementation plan of an automated decision-making system as required by the directive (see subsection 6.1.2 of the directive).

Engage legal services early in order to meet the directive's requirement to consult with institutional legal services (see subsection 6.3.8 of the directive) and maximize their value. Legal services can provide advice on the following:

- the requirements of the explanation for decisions (see subsection 6.2.3 of the directive)
- how to answer certain AIA questions
- recourse options that need to be available (see subsection 6.4.1 of the directive)
- other issues

In order to meet transparency requirements (see subsections 6.1.4 and 6.2 of the directive) and pursuant to the *Directive on Open Government*, consider in advance what documents and data will be published. The AIA's "De-Risking and Mitigation Measures" section suggests several publications to mitigate risks and increase transparency and public trust. Reviewing these materials will also help ensure that official languages and accessibility are considered from the beginning.

Execution phase

Working with suppliers

In the event that part of the implementation is contracted to suppliers, consider sharing the directive with them so that they are aware of the department's obligations. It is the department's responsibility to ensure that the requirements of the directive are met.

In drafting the statement of work, consider including requirements to ensure the supplier's participation in compliance processes, as appropriate. For example:

- Have the supplier participate in completing the AIA (see subsection 6.1.1 of the directive) so that they can be informed of the potential impacts of the system and advise on the feasibility of certain mitigation measures proposed.
- Have the supplier participate in the peer review (see subsection 6.3.4 of the directive). Doing so will provide additional information on the system design, testing conducted to minimize undesired outcomes, training data, and other aspects.

Finally, note that some of the directive's requirements directly impact the clauses that must be present in the contract. Ensure that the requirements for access to components are adequately covered in the contract or licence (see subsection 6.2.5 of the directive).

Model selection

The section on model selection of the AIA is relevant only if machine learning is used in the automation of decision-making.

Being able to explain how decisions are made is critical (see subsection 6.2.3 of the directive). If generating this explanation to the client requires understanding how an artificial intelligence (AI) arrived at its result, it is important that the AI model itself be interpretable. Having an easily interpretable model can also greatly simplify testing and verifying of the system, including assessing bias. With recent impressive computational improvements, there are many techniques to achieve this. It is important that the way an explanation is derived for decisions is considered when selecting and designing a machine-learning model.

By their design, neural networks and deep learning come with greater challenges in providing an easily intelligible explanation. On the other hand, it is simpler to interpret the results of algorithms such as optimized rule lists, sparse linear models with integer coefficients and sparse decision trees, and their accuracy can be comparable in many situations. The pros and cons of each are often application-specific. Favour the simplest model that will provide the performance, accuracy, interpretability and lack of bias required.

Terminology in the field is not standardized. The terms “interpretability” and “explainability” are sometimes used interchangeably. Interpretability is the ability to present in understandable terms to a human how a prediction was derived by inspecting the model itself. In other words, interpretability refers to the resulting prediction being readily discernable directly from the inputs, by a human. This is highly desirable.

Explainability is a set of techniques, often applied to black-box models, to explain a prediction. In more complex cases, it may refer to the use of a second, simpler model that makes very similar predictions to the original production model to provide a clearer understanding of that prediction. Because the two models may yield different predictions in some cases, the resulting explanation can be misleading. Additional assessments may be required when the simpler model produces different predictions. Perhaps more importantly, be aware that the simpler model is only an approximation and may suggest explanations that are unrelated to what is actually going on in the original model.

4.6 Cyber security

4.6.1 Description and associated requirement

This section provides detailed guidance on cyber security with respect to requirements of the *Policy on Service and Digital* and the *Directive on Service and Digital*. However, cyber security is to be considered under every theme of this guideline to ensure that Government of Canada and departmental information and data, applications, systems and networks are secure, reliable and trusted.

Cyber security refers to the body of technologies, processes, practices, and response and mitigation measures designed to protect electronic information and information infrastructure from mischief, unauthorized use or disruption.

To ensure that cyber security is appropriately managed in the Government of Canada, the *Policy on Service and Digital* requires that deputy heads establish clear reporting responsibilities for cyber security.

Requirement for departments under the policy
Deputy heads are responsible for: 4.4.2.7 Clearly identifying and establishing departmental roles and responsibilities for reporting cyber security events and incidents, including events that result in a privacy breach, in accordance with the direction for the management of cyber security events from the CIO of Canada.

The requirements of the *Directive on Service and Digital* outline how the designated official for cyber security is required to respond to and manage cyber security events in the organization. To provide timely and efficient management of cyber security events and incidents, an incident management program must have:

- supporting services and activities
- strategic leadership in place to ensure informed decision-making

Furthermore, ensuring that cyber security requirements and appropriate measures are applied to protect IT infrastructure will enable the trusted delivery of internal and external programs and services.

Requirements for departments under the directive
The **designated official for cyber security, in collaboration with the departmental CIO and chief security officer** as appropriate, is responsible for: 4.4.2.1 Ensuring that cyber security requirements and appropriate measures are applied in a risk-based, life-cycle approach to protect IT services, in accordance with the *Directive on Security Management*, Appendix B: Mandatory Procedures for Information Technology Security Control. 4.4.2.2 Ensuring departmental plans, processes and procedures are in place for responding to cyber security events and reporting of incidents to the appropriate authorities and affected stakeholders, in accordance with the *Government of Canada Cyber Security Event Management Plan*. 4.4.2.3 Undertaking immediate action within the department as directed to assess impacts, including whether there has been a privacy breach, and implement mitigation measures in response to cyber security events. 4.4.2.4 Liaising with the access to information and privacy office in the department and the Office of the Privacy Commissioner when there has been a material privacy breach.

4.6.2 Why is this important?

Digital technologies and the Internet are increasingly important to innovation and economic growth. Strong cyber security is critical to Canada's competitiveness, economic stability and long-term prosperity as a digital nation.

The requirements related to this theme ensure that cyber security and incidents events are addressed in a consistent, coordinated and timely fashion across the Government of Canada. They also ensure that appropriate cyber security measures are applied in a risk-based, life-cycle approach. Taken together, all cyber security requirements serve to enable sustainable, secure, resilient, government-wide infrastructure that supports the trusted delivery of internal and external programs and services. Furthermore, cyber security enables the delivery of trusted and secure services that Canadians want and expect.

4.6.3 Considerations in implementing the requirements

When identifying and establishing roles and responsibilities for reporting cyber security events and incidents, the chief security officer (CSO) should consider section 5 of the Government of Canada Cyber Security Event Management Plan: 2019 update (GC CSEMP), in accordance with subsection 4.1.6 of the *Directive on Security Management*. The GC CSEMP provides an operational framework for managing cyber security events (including cyber threats, vulnerabilities or security incidents) that impact or threaten to impact the Government of Canada's ability to deliver programs and services to Canadians.

Following are some considerations for the designated official for cyber security in implementing the directive requirements above to ensure that cyber security requirements and appropriate measures are applied in a risk-based, life-cycle approach to protect IT services, in consultation with the departmental CIO and CSO.

Apply a risk-based approach

- Understand business context and stakeholder needs.
- Identify and categorize information based on the degree of injury that could be expected to result from a compromise of its confidentiality, integrity and availability. For more information, consult the Standard on Security Categorization of the *Directive on Security Management*, as well as the security categorization tool.
- Evaluate how new program and systems will impact the personal information of Canadians.
- Integrate cyber security into organizational risk management processes.

Design for security and privacy

- Make it easy for users to do the right thing, balancing ease of use and security.
- Embed security and privacy principles throughout the design of services and systems. For specific information on considerations at the design stage, refer to subsection 4.1 of this guideline.
- Design systems that are resilient to both attack and failure.
- Perform threat modelling and prioritize cost-effective security measures to reduce cyber threats and protect personal information.
- Limit services exposed and information exchanged to the minimum necessary. For more information on privacy requirements, refer to subsection 3.6 of this guideline.
- Ensure that systems adequately protect data at rest and data in transit using approved security measures such as cryptography.

Build secure systems and services

- Address security requirements and adjust as necessary throughout all the stages of the system development life cycle in accordance with the *Directive on Security Management*, Appendix B: Mandatory Procedures for Information Technology Security Control.
- Build out services and systems using industry best practices (for example, SAFECode Fundamental Practices for Secure Software Development, ISO/IEC 27034 and Open Web Application Security Project (OWASP).
- Restrict access to systems and services to users based on the principles of least privilege, need to know and segregation of duties.

- Implement user and system authentication and authorization before access is granted, including digital identity and the use of multi-factor authentication for important accounts or services. Leverage enterprise services such as Government of Canada trusted digital identity solutions that are supported by the Pan-Canadian Trust Framework. For more information, refer to subsection 4.7 of this guideline for digital identity considerations.
- Implement measures to support "hardening" (for example, disabling of all non-essential services, ports or functionality) of systems, devices and applications.
- Perform security assessment and authorization of information systems or services before approving them for operation.

Ongoing maintenance and monitoring

- Ensure that threat assessments and defensive measures are regularly reviewed and updated accordingly.
- Enable event logging on systems and applications and audit sensitive actions or data exchange/access and monitor for signs of malicious or anomalous activity.
- Continually manage vulnerabilities and promptly apply security-related patches and updates.
- Prepare to respond to and recover from successful attacks. Establish an incident management plan in alignment with the GC CSEMP.
- Put in place a privacy breach plan. In the event of a privacy breach, undertake immediate action as outlined in the *Directive on Privacy Practices* and the *Guidelines for Privacy Breaches*. For more information, refer to subsection 3.6 of this guideline.

Additionally, tools and templates are available to help integrate security throughout the system life cycle and design and operations of a service:

- Government of Canada Enterprise Security Architecture (GC ESA) Artifact Repository
- Security Playbook for Information System Solutions

4.7 Digital identity

4.7.1 Description and associated requirement

As outlined in the *Directive on Identity Management*, a trusted digital identity is an electronic representation of an individual that is used to access services and carry out digital transactions with trust and confidence. Put simply, digital identity confirms that you are who you say you are in an online context.

In addition, a trust framework is a set of agreed on definitions, principles, conformance criteria, assessment approach, standards and specifications, as outlined in the *Directive on Identity Management*. Furthermore, it is a framework of rules that supports the use and acceptance of digital identities by defining and assessing a set of processes (for example, identity validation, identity resolution) that can be mapped to business processes and independently assessed using conformance criteria.

By leveraging trust frameworks, departments support a federated approach to digital identity that facilitates the use and acceptance of trusted digital identities between various levels of government and the private sector. Trust frameworks also ensure technical interoperability and enable compatibility with emerging technologies (for example, blockchain-based identity management approaches, zero-trust networks and digital wallets).

The *Policy on Service and Digital* requires that deputy heads align their departmental approaches for identity assurance with enterprise-wide expectations to support interoperability.

Requirement for departments under the policy
Deputy heads are responsible for: 4.4.2.8 Managing departmental approaches for identity assurance and accepting trusted digital identities to support interoperability by using approved trust frameworks.

4.7.2 Why is this important?

Canadians expect simple, fast and convenient access to services anytime, anywhere, on any device. Digital identity can be used to accelerate these efforts. Currently, users are required to have separate interactions across different platforms in order to access services, which often results in multiple in-person visits and/or usernames and passwords. This process is time-consuming and often unnecessary, as users usually already possess a digital identity with another department or other level of government (for example, provincial or territorial) that is trusted and recognized by the Government of Canada.

Transforming services to meet these expectations begins with users' digital identity, as once an identity is established and verified, all subsequent activities can occur. Put simply, digital identity is the foundation of service delivery and moving more services online. In addition, digital identity provides users with more choice and control over their digital lives as they choose which credential or trusted digital identity to authenticate themselves with and access the services they need. Leveraging approved trust frameworks would provide users with the choice to use, for example, their provincial trusted digital identity, GCKey or banking credential to access federal services.

This policy requirement ensures effective identity management and allows digital identities to be managed consistently and collaboratively across the Government of Canada and with other jurisdictions. To that end, in managing departmental approaches for digital identity by leveraging approved trust frameworks, deputy heads can integrate standardized identity levels of assurance and enable greater interoperability that is consistent with a government-wide, pan-Canadian approach.

4.7.3 Considerations in implementing the requirement

Following are some implementation considerations and useful resources:

- Integrate standardized identity and credential assurance levels into programs, activities and services, as required, as outlined in:
  - Standard on Identity and Credential Assurance
  - *Guideline on Defining Authentication Requirements*
  - *Guideline on Identity Assurance and the Government of Canada Guidance on Using Electronic Signatures*
- Leverage the Public Sector Profile of the Pan-Canadian Trust Framework (PSP-PCTF) in managing departmental approach for identity assurance and accepting trusted digital identities, where required. The PSP-PCTF is a rule framework that supports the use and acceptance of digital identities from the Government of Canada and other jurisdictions (for example, provinces and territories).
- Use mandatory enterprise services for identity management, credential management and cyber authentication, as outline in subsection 4.1.9 of the *Directive on Identity Management*.
- Ensure compatibility with the Cyber Authentication Technology Specification.
- Ensure that privacy and security-related considerations are addressed from beginning to end. For more information, refer to subsection 3.6, subsection 4.1 and subsection 4.6 of this guideline.

5. Supporting workforce capacity and capability

The *Policy on Service and Digital* sets out requirements to ensure departmental workforce awareness, capacity and capability as it relates to service, IT, information, data and cyber security to better meet departmental priorities. The policy also sets rules on how departments can meet the needs of a digital government and client expectations for services by providing and promoting talent management and community development strategies for the service, information, IT and cyber security functional communities.

It is important to note that all activities related to managing the government workforce are to be carried out in accordance with Treasury Board policy instruments related to people management.

Among the expected outcomes of the *Policy on Service and Digital* is that leadership and community strategies support workforce capacity and capability for a digitally enabled and skilled public service.

5.1 Workforce awareness, capacity and capability

5.1.1 Description and associated requirements

Departments that regularly implement activities that foster workforce awareness, capacity and capability lay the foundation for meeting the needs of clients and achieving program outcomes. At the departmental level, deputy heads are responsible for workforce awareness, capacity, and capability to meet departmental and enterprise service, information, data, IT and cyber security requirements.

Requirement for departments under the policy
Deputy heads are responsible for: 4.5.2.1 Ensuring departmental workforce awareness, capacity, and capability to meet departmental and enterprise service, information, data, IT, and cyber security requirements.

Workforce capacity pertains to departments having the financial resources, employees and systems they need to deliver and meet the objectives of the organization. Workforce capability pertains to employees having the resources, tools, relationships, training, education and supervisory support to enable them to apply knowledge and skills in their day-to-day work. Awareness, on the other hand, pertains to employees knowing how digital transformation impacts their day-to-day work and understanding the considerations related to operating in the digital era, whether it is in delivering a service to Canadians, establishing a program, managing departmental operations or any other activity. In short, workforce awareness is about understanding how we do business in the digital era.

5.1.2 Why is this important?

Enhanced workforce awareness, capacity and capability result in better service experiences, improved program outcomes and operations.

There are many benefits to achieving increased workforce awareness, capacity and capability, including the following:

- increased ability for the Government of Canada to adapt to change, which is especially important for the areas of management of service design and delivery, IT, information, data and cyber security, given the pace of change in these areas
- enhanced awareness of stakeholders and users and their expectations in an ever-changing world
- increased ability to attract and retain talent as employees develop a greater sense of belonging, self-worth and dignity due to their enhanced abilities
- enhanced employee productivity and autonomy
- improved ability to find innovative and creative solutions, even for new problems, as a result of increased confidence in base knowledge and skills needed to carry out everyday tasks

5.1.3 Considerations in implementing the requirement

Having a workforce that has the right competencies (knowledge and skills) is important to achieve enhanced workforce awareness, capacity and capability. The term “knowledge” refers to knowledge about the specific area of management (for example, service officers having knowledge related to the service that they offer), whereas the term “skill” refers to the aptitudes needed to undertake the work (for example, service officers having the communications skills to interact with clients). Although not exhaustive, the table below lists some knowledge and skills related to the fields of service design and delivery, IT, information, data literacy and cyber security.

Service design and delivery, IT, information, data literacy and cyber security knowledge and skills

Component	**Description**
Service	Knowledge of the following: • departmental mandate, objectives and priorities • departmental products, services and partners • the program that the service supports • related programs and services for clients (for example, those provided by other departments and other levels of government) • any applicable service pledges, commitments and standards • client needs and expectations • service design and delivery concepts and techniques • existing and emerging client-engagement tools, management tools, technology and applications • privacy, identity management and security practices that support the service • official languages requirements that must be met when providing the service

Component	**Description**
	Ability to do the following: • demonstrate an understanding of own role and responsibilities, and those of other parties involved in providing the service • follow applicable Government of Canada and departmental policies, regulations and procedures relating to service • use effective interpersonal communication techniques to identify client needs (for example, questioning, active listening) and to maintain positive relationships • demonstrate a helpful, caring and professional attitude when serving clients • assess a situation and apply problem-solving techniques to achieve positive client-service outcomes • resolve client service issues, including urgent ones, in a timely manner • seek feedback from clients to improve the quality and efficiency of services • work collaboratively to provide integrated services to clients • provide service that is consistent with organization's values • use language and actions that show respect for clients
Data literacy	Knowledge of the following: • **conceptual:** basic understanding of the concept of data and its evolving role in supporting policy, programs and services to Canadians • **operational:** knowledge of the ways in which data is managed throughout its life cycle, from collection through to disposition • **analytical:** knowledge of quantitative, qualitative, and/or mixed techniques of manipulating data to extract useful information from it, as well as of the tools needed to conduct such manipulations • **interpretative:** knowledge of how to interpret the results of data analyses in a business context and assess their applicability in that context, including knowledge of relevant policy and legislation Ability to do the following: • **Conceptual** ○ **Communication:** Ability to communicate about data issues within and across functional communities ○ **Planning:** Ability to identify data gaps or needs in the context of a project, problem or initiative • **Operational**

Component	Description
	○ **Life-cycle management and governance:** Ability to collect, store, organize and manage data assets throughout their life cycle, according to applicable retention and disposition schedules and relevant policy and legislation • **Analytical** ○ **Quantitative analysis:** Ability to use statistical and/or mathematical methods to analyze and derive insights from data, using tools such as SAS and/or programming languages such as R, Python and JavaScript, among others ○ **Qualitative analysis:** Ability to analyze the content, narrative, assumptions and other qualitative dimensions of data and draw conclusions on that basis, including through coding techniques ○ **Mixed-method analysis:** Ability to combine multiple methods of data analysis to derive insights from data • **Interpretive** ○ **Data consumption:** Ability to use the information resulting from data analyses to make informed decisions or support other aspects of a business line (involves assessing the applicability and relevance of the information to the purpose it is being considered for, and determining its reliability, validity and veracity, among other dimensions of fitness)
Information and data management	Knowledge of the following: • **general knowledge and experience:** knowledge of Government of Canada and departmental information and data management rules, tools and resources, including information and data governance • **information and data management practices:** information and data management policy development and implementation, information and data management operational processes, information and data protection and security procedures, and compliance Ability to do the following: • **focus on clients:** identify and respond to current and future client needs, provide service excellence to internal and external clients, and negotiate and reach consensus with clients • **communicate:** listen actively to others and present appropriate information clearly and concisely

Component	Description
	• **manage change:** manage uncertainty and develop the networks and personal relationships required to facilitate change and achieve desired business outcomes • **be aware of the organization and its environment:** understand the business, structure and culture of the organization, as well as the political, social, economic and technological environments • **thinking analytically:** interpret, link and analyze information in order to understand issues • **plan and organize:** define, plan and organize activities, as well as resources, to achieve optimal results • **Identify and analyze information and data management requirements:** identify, analyze, assess and define the information and data management rules, tools and resources required to manage information and data to ensure the effective and efficient conduct of business and the delivery of programs and services • **apply implement and use information and data management rules, tools and resources:** apply, implement, use and provide advice and guidance on information and data management rules, tools and resources to address information and data management requirements • **design and develop information and data management rules, tools and resources:** design, develop and recommend the information and data management rules, tools and resources needed to meet information and data management requirements
Information technology	When it comes to the IT, there are a number of resources about the CIO suite of competencies available, including competency dictionaries, which are profiles, including information on knowledge and skills, available for various streams, such as: • planning • enterprise architecture • IT security • infrastructure/operations • application development • database and data administration • IT business line support services

Component	Description
	These competency dictionaries and profiles describe successful performance as observable, measurable behaviours and ensure that there is common, universally understood terminology linked to performance expectations.
Cyber security	In addition to the knowledge and skills identified in the IT security portion of the CIO suite of competencies, the following cyber security-related knowledge and skills are important for employees working in the field: • knowledge of the following: ○ Government of Canada and departmental policies and instruments relating to cyber security and IT security ○ the organization's business context and threat environment ○ the organization's overall security posture (for example, state of authorities to operate the various systems, plans of action and mitigation) • ability to do the following: ○ solve problems: attacks can emerge at any time, and teams must be ready to change course and solve problems quickly ○ have an agile and flexible mindset: strong teams can shift priorities to meet the challenge of the day ○ be learning-oriented: to respond to new threats, teams need to always learn new skills and methodologies to secure systems ○ collaborate: security has to be an enabler working with business owners and projects, from the outset

Actions in support of increased workforce awareness, capacity and capability

There are a number of methods and tools (formal and informal) that can be used to enhance workforce awareness and capability. Methods include training, information or orientation sessions, videos, information provided via internal collaborative tools, manager debriefs, account sign-on notifications and electronic newsletters.

There are a few specific actions that departments may want to take to support the development of workforce awareness, capacity and capability. These actions may include the following:

Upon commencement of employment

- Provide toolkits that include information about government-wide and departmental policy requirements relating to the area of management.

- Hold briefing sessions to ensure that employees have the knowledge they need to perform their job well.
- Distribute information about organizational structure and the governance structure to ensure understanding of decision-making process in support of departmental priorities.
- Provide employees with contact information of those who are involved in activities that relate to their work in order to make linkages and increase awareness on interdependencies between areas of management.

On a regular basis

- Support training and certification opportunities.
- Integrate learning opportunities into performance agreements and learning plans, including talent management.
- Offer informal mentoring and coaching opportunities.
- Organize departmental events and networking opportunities to share information and knowledge.
- Recognize achievements during team or other meetings.
- Develop, maintain and share a list of best practices.
- Raise awareness and encourage experimentation with new approaches.
- Review the learning approach or plan to ensure that it remains up to date.

Resources

In addition to its general course offerings on information management, IT, service excellence and other topics, the Canada School of Public Service (CSPS) is home to the Digital Academy. This academy offers a curriculum that supports public servants at all levels in modernizing their operations to deliver the kind of digital services that people expect. Some learning opportunities are more general in nature, while others are specialized.

The Digital Academy also hosts events as part of the “Let’s Talk Digital” and “Digital Acumen” series. These events are posted in the CSPS Events calendar. To learn about the Digital Academy’s offerings, subscribe to the Digital Academy newsletter, follow the Digital Academy on Twitter, or email the Digital Academy directly if you have specific questions.

5.2 Chief information officer talent management and community development initiatives

5.2.1 Description and associated requirements

At the **government-wide level**, the CIO of Canada is responsible for providing enterprise-wide leadership on the development and sustainability of the information and IT functional community by using talent management and community development strategies.

This requirement is mirrored at the **departmental level** where departmental CIOs are required to do the same for their organization. To reinforce this, the deputy head is responsible for supporting the CIO of Canada's enterprise-wide talent management and community development initiatives.

Requirement for TBS under the policy
The **CIO of Canada** is responsible for: 4.5.1.1. Providing enterprise-wide leadership on the development and sustainability of the information and IT functional community by using talent management and community development strategies.

Requirements for departments under the policy
Deputy heads are responsible for: 4.5.2.2. Supporting the CIO of Canada's enterprise-wide talent management and community development initiatives.

Requirements for departments under the directive
The **departmental CIO** is responsible for: 4.5.1.1. Providing functional leadership in the department on the development and sustainability of the IT and information communities through talent management and community development strategies.

5.2.2 Why is this important?

There are a number of reasons why the development of community development strategies (which includes talent management) for the information and IT functional communities is important. Benefits of such strategies include the following:

- increased opportunities to bring people together to ensure that the communities have the resources and tools they need to carry out their functions

- increased collaboration and sharing of information, ensuring that department that face similar issues can learn from one another
- increased awareness of local, national and international trends that pertain to information and IT
- enhanced relationship-building and sense of belonging, resulting in mobility among employees working within the information and IT communities

5.2.3 Considerations in implementing the requirements

In their work on community development strategies, departments are encouraged to keep abreast of government-wide efforts. The CIO Suite of Generic Products provides the tools necessary to support an integrated and strategic approach to enterprise and organizational human resources management, as well as employee career planning and personal development in the field of IT and information management. The suite was developed by the community, for the community, and it continues to evolve to meet the people management needs of all community members. The suite of products includes a number of resources to support the IT and information management communities. Resources are related to various potential components of community development strategies, such as:

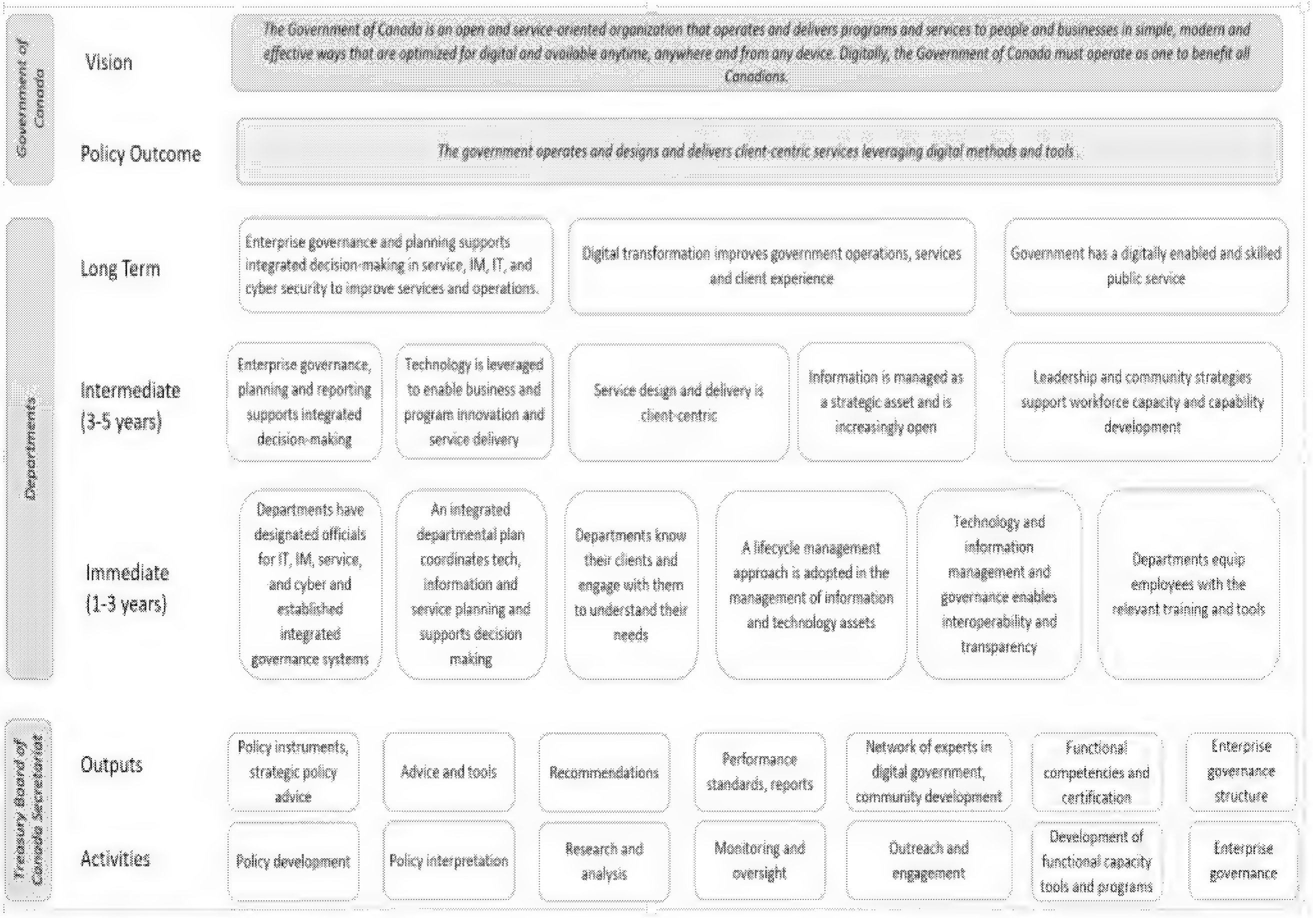
- talent management
- competencies
- recruitment and staffing
- other useful information

To participate in the information management and IT community, consult the IM-IT Functional Community (IFC) GCconnex page (available only on the Government of Canada network).

In developing community development strategies, departments need to ensure that appropriate linkages are made with existing human resources programs in their organization.

Appendix A: *Policy on Service and Digital* Logic Model

The logic model provides a list of outcomes that departments are expected to achieve by implementing the requirements of the *Policy on Service and Digital*.



Government of Canada

Vision

The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device. Digitally, the Government of Canada must operate as one to benefit all Canadians.

Policy Outcome

The government operates and designs and delivers client-centric services leveraging digital methods and tools.

Departments

Long Term

Enterprise governance and planning supports integrated decision-making in service, IM, IT, and cyber security to improve services and operations.

Digital transformation improves government operations, services and client experience

Government has a digitally enabled and skilled public service

Intermediate (3-5 years)

Enterprise governance, planning and reporting supports integrated decision-making

Technology is leveraged to enable business and program innovation and service delivery

Service design and delivery is client-centric

Information is managed as a strategic asset and is increasingly open

Leadership and community strategies support workforce capacity and capability development

Immediate (1-3 years)

Departments have designated officials for IT, IM, service, and cyber and established integrated governance systems

An integrated departmental plan coordinates tech, information and service planning and supports decision making

Departments know their clients and engage with them to understand their needs

A lifecycle management approach is adopted in the management of information and technology assets

Technology and information management and governance enables interoperability and transparency

Departments equip employees with the relevant training and tools

Treasury Board of Canada Secretariat

Outputs

Policy instruments, strategic policy advice

Advice and tools

Recommendations

Performance standards, reports

Network of experts in digital government, community development

Functional competencies and certification

Enterprise governance structure

Activities

Policy development

Policy interpretation

Research and analysis

Monitoring and oversight

Outreach and engagement

Development of functional capacity tools and programs

Enterprise governance

The outcomes shown in the logic model will be further articulated in future guidance and tools to support departments from a performance measurement perspective in their transition toward a digital government.

Appendix B: Client-Centric Services

This appendix provides advice on what constitutes a service under the *Policy on Service and Digital*. Although the Treasury Board of Canada Secretariat (TBS) can provide assistance to departments in determining their services, departments are ultimately responsible for determining what constitutes or does not constitute a service, based on their own specific operational context.

B.1 Key terms and concepts

B.1.1 What is a service?

A service is the provision of a specific final output that addresses one or more needs of an intended recipient and contributes to the achievement of an outcome.

Definitions and explanations of the key terms contained in the definition of service are outlined in the following.

Final (service) output

- A unit of value that is delivered directly to a client by a service.
- An output can be tangible (for example, a passport, a licence, a payment, a permit) or intangible (for example, information, advice), and one service can produce both tangible and intangible outputs. The frequency and time frame of outputs may also vary: some might be delivered to a client only once in a period of years (for example, a passport), and others might be delivered regularly over a period of time (for example, employment insurance payments). Some final outputs might take many years to receive (for example, the certification of a new type of aircraft or the granting of a patent).

Need

- A requirement or desire of a target group that a program has a mandate to satisfy or reduce.
- The starting point for both programs and services is the identification of a need. Needs are met by a program, which has the mandate and resources to address those needs. A program is delivered through one or many services. Needs are usually addressed by the output of a service.

Recipient (or client)

- Individuals, businesses or their representatives served by or using services provided by the Government of Canada. When describing recipients' interactions with information technologies, clients can be referred to as users.

Outcome

- An external consequence attributed, in part, to an organization, policy, program or initiative. Outcomes are not within the control of a single organization, policy, program or initiative; instead they are within the area of the organization's influence. Outcomes are usually further qualified as immediate, intermediate, or ultimate (final), expected, direct, etc.

- To differentiate between outputs and outcomes, the following example is helpful. The Department of Employment and Social Development Canada, through Service Canada, provides passport services in Canada on behalf of the Passport Program and has the authority to issue Canadian passports. The output of this service is a passport. The outcome is the ability for Canadians to travel abroad.

B.1.2 Critical services

A critical service is a service whose compromise in terms of availability or integrity would result in a high or very high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada. Refer to the *Policy on Government Security* for more information and guidance.

Contact your department's security functional specialist for business continuity management. This specialist inputs critical service data into the Critical Services module of the Clarity Tool.

B.1.3 How to identify services?

Service Identification Tool

Some services are easy to identify; others are not and require careful consideration and discussion. For assistance in determining whether an activity or a series of activities is a service, consider using the Service Identification Tool provided below. Although this tool provides general guidance, it is up to departments to make the final determination.

Also consult the table on Service Output Types, as it identifies a broad range of services, including regulatory authorizations and penalties, that are also considered to be services.

Some key questions to ask when determining whether an activity is a service (see the Service Identification Tool diagram) are as follows:

1. Does a specific activity result in a final output to recipients or clients?
2. Are there multiple clients and recipients?
3. Is the final output produced repeatedly?
4. Are the activities contributing to the achievement of an outcome that is independent of any other service?
5. Does the activity meet the "materiality test" of supporting the well-being of individuals or the effective operation of organizations?

If the answer to most of these questions is yes, then the activity is likely a service and should be included in the service inventory.

When identifying services, keep the following in mind:

- an applicant may not always successfully obtain a final output (for example, a request for funding)
- a service does not always require that a service provider interact directly with a recipient (for example, weather forecast)

- a recipient may not always request the service (for example, tax audit, mandatory inspection)
- if the activity has service standards and entails an application process, it is likely a service

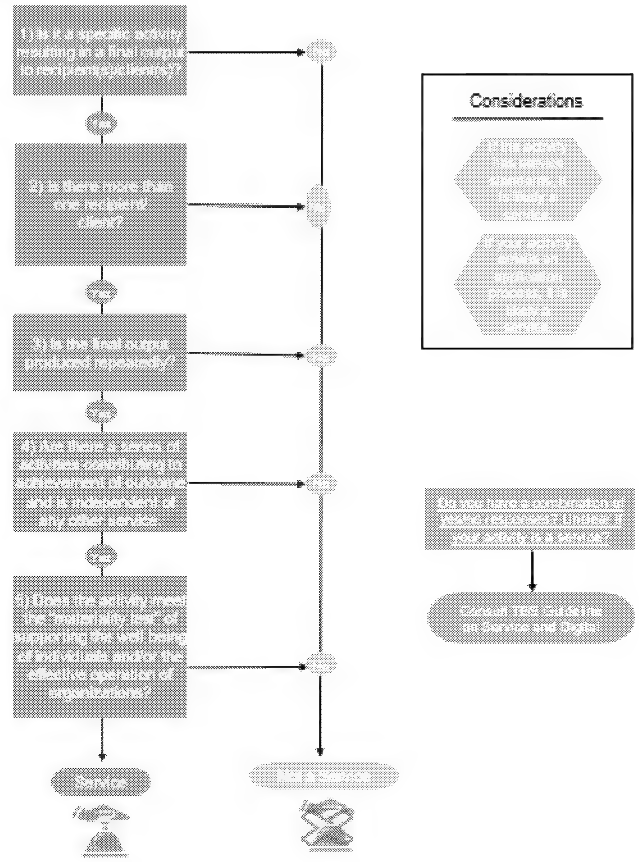
Service Identification Tool

This Service Identification Tool helps identify if an activity is a service. While this tool provides general guidance, it is up to departments to make the final determination.

A service is the provision of a specific or final output that addresses one or more needs of an intended recipient and contributes to the achievement of an outcome.

Getting started: As a first step, departments are encouraged to review their Departmental Plan, program inventory and web presence to identify potential services. Once a list of potential services is established, use the following tool to confirm if your activity is indeed a service.

Is your activity a service?



1) Is it a specific activity resulting in a final output to recipient(s)/client(s)?

2) Is there more than one recipient/ client?

3) Is the final output produced repeatedly?

4) Are there a series of activities contributing to achievement of outcome and is independent of any other service.

5) Does the activity meet the "materiality test" of supporting the well being of individuals and/or the effective operation of organizations?

Service

Not a Service

Considerations

If the activity has service standards, it is likely a service.

If your activity entails an application process, it is likely a service.

Do you have a combination of yes/no responses? Unclear if your activity is a service?

Consult TBS Guideline on Service and Digital

When identifying services, keep the following in mind:

- A recipient may not always successfully obtain a final output.
- A service does not always require that a service provider interact directly with a recipient.
- A recipient may not always request the service (for example, tax audit, mandatory inspection).

The following three examples illustrate how to determine whether an activity is a service, using the Service Identification Tool.

Example 1: AgriStability

Department: Agriculture and Agri-Food Canada

Description: Provides funding (based on the selected level of protection) when producers' production margins fall below their reference margin. For further details, consult the AgriStability web page.

Service Test Tool Example 1: AgriStability

Questions	**Analysis**	**Yes/No**
1. Does a specific activity result in a final output to recipients or clients?	The funding is the final product of the service and is what farmers were seeking when they originally applied and paid for the service. The distribution of funds is the final output.	Yes
2. Are there clearly defined clients or recipients?	The clients are farmers.	Yes
3. Are there multiple clients and recipients?	There are many farmers who could use this service.	Yes
4. Is the final output produced repeatedly?	The funding is given repeatedly and in different years.	Yes
5. Are the activities contributing to the achievement of an outcome that is independent of any other service?	AgriStability does not require additional activities or processes to ensure that it contributes to a program outcome. It also does not depend on other services.	Yes
6. Does the activity meet the "materiality test" of supporting the well-being of individuals and/or the effective operation of organizations?	It provides funding when producersè production margins fall below their reference margin by more than 30%.	Yes
Conclusion: This is a service.		

Example 2: Icebreaking

Agency: Canadian Coast Guard

Description: Supports economic activities by assisting commercial vessels to voyage ice-covered waters. For further details, consult the Canadian Coast Guard's Icebreaking web page.

Service Test Tool Example 2: Icebreaking Program

Questions	Analysis	Yes/No
1. Does a specific activity result in a final output to recipients or clients?	The icebreaking and the protection that goes along with icebreaking are what the services that the client has requested and paid for. It is the final output.	Yes
2. Are there clearly defined clients or recipients?	Potential clients could be shipping companies or the general public.	Yes
3. Are there multiple clients and recipients?	This service is provided to many clients: commercial vessels, Arctic residents, port operators and the general public.	Yes
4. Is the final output produced repeatedly?	The ice is cleared many times during the winter, year after year.	Yes
5. Are the activities contributing to the achievement of an outcome that is independent of any other service?	Icebreaking does not depend on other services.	Yes
6. Does the activity meet the "materiality test" of supporting the well-being of individuals and/or the effective operation of organizations?	It supports economic activities by assisting commercial vessels to voyage efficiently and safely through or around ice-covered waters.	Yes
Conclusion: This is a service.		

Example 3: Canada Benefits

Agency: Service Canada

Description: The Canada Benefits website is a tool that provides government-wide information about benefit programs and services for individuals. A number of government departments developed this website, including the Canada Revenue Agency, the Canada Mortgage and Housing Corporation, Canadian Heritage, Employment and Social Development Canada, the Department of Justice Canada, Service Canada, and Veterans Affairs Canada. The site also contains information on programs administered by Immigration, Refugees and Citizenship Canada and all of Canada's provinces and territories.

For further details, consult Service Canada's Canada Benefits web page.

Service Test Tool Example 3: Canada Benefits website

Questions	Analysis	Yes/No
1. Does a specific activity result in a final output to recipients or clients?	The website is a tool that identifies various benefit programs and services based on target group and life events. It provides links to other websites. It is therefore an intermediate output, rather than a final output to a client.	No
Conclusion: This is not a service.		

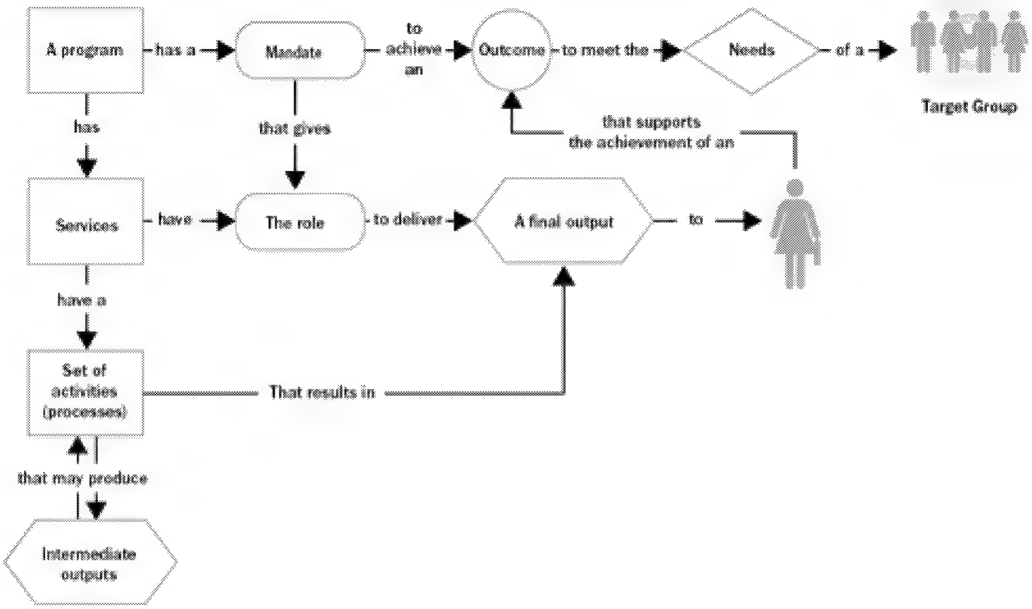
B.1.4 Programs vs. services

Programs provide the context for determining the services to be delivered. Programs are generally delivered through services, which contribute to achieving program objectives.

Most departments have already identified their outcomes, or expected results, in their Departmental Results Framework, which are to be reflected in their Program Inventory as required by the *Policy on Results*. Services contribute to achieving those expected results (outcomes).

An understanding of services first requires knowledge of the context in which they operate. Services are a component of a program that contributes to a specific set of outputs. Services deliver a final output to recipients, or clients, to support the achievement of the outcome. Services are composed of activities (processes) that lead to the final output. Figure 1 illustrates this context.

Figure 1: Context in which services operate



Text version: Figure 1: Context in which services operate

This is a graphical representation of the context within which Government of Canada services operate that includes the key terms from the definition of service. The image shows that departmental programs have the mandate to achieve an outcome to meet the needs of a target group. Services deliver a final output to recipients, or clients, to support the achievement of the outcome. Services are composed of activities (processes) that lead to the final output.

Final outputs vs. intermediate outputs

When determining whether an activity is a service, it is helpful to ask whether the activity produces an intermediate output or a final output to a client. Examples include the following:

- The provision of a regulatory permit or certificate usually constitutes a final service output. The denial of a permit can also be the final service output. The approval or denial of the permit completes the series of activities from the client's perspective.
- Information posted on the Government of Canada website about how to apply for a permit or certificate constitutes an intermediate output, because the client must complete subsequent steps before being issued the permit.
- Advice or information from a call centre agent is the final output of a service when the client does not have to complete subsequent activities.
- The issuing of a new passport constitutes the final output from a service, but accepting a completed passport application does not because that activity does not conclude the interaction between the service provider and the recipient, and it does not result in a final output. In this case, the denial of a passport can be considered the final output of the service.

Relationship between activities and services

A service consists of a series of activities (processes) that result in a single final output for the recipient (or client). Each activity is not considered an individual service even though it might produce intermediate outputs.

Consider a scenario where a business owner requires a permit or certificate from the Government of Canada to be able to proceed with a specific action on business premises. The series of activities may involve the following:

- providing an online application on the Government of Canada website for use by the business owner to apply for the permit or certificate
- responding to a call from the business owner who may need additional information to complete an application; responding to this call supports the service (1-800 call centre)
- receiving and processing an application, which may include assessing the application against established eligibility criteria
- inspecting the business premises to ensure that it meets requirements
- issuing the permit or certificate, which is the culmination of the series of activities and is the final output of the service

B.1.5 Grants and contributions as a service

The administration of grants and contributions (Gs&Cs) usually constitutes a service, as they provide a final output (funding), except in the case of statutory transfer payments made to other governments or other organizations (for example, fiscal equalization, membership dues to the North Atlantic Treaty Organization).

Gs&Cs meet the definition of a service in that there is a final output (funding), there is a need (funds), there is a recipient, and it supports an outcome or public policy goal (the reason the government is providing the G&C). Service standards are often applied to the administration of Gs&Cs.

For more information on Gs&Cs, consult the *Policy on Transfer Payments*.

B.1.6 Information or data as a service

Information or data is a service when it constitutes a final output to a client and when it has the other elements contained in the definition of service (that is, need, recipient and outcome), for example, a weather forecast or labour or market statistical information.

Addressing the following considerations can help in assessing whether information or data is a service.

- Does the provision of information or data represent a final output?
    - Is the information or data the final output, or is it part of a larger process that leads to a final output? The greater the sense that the information or data is the final output, the greater the likelihood it is a service. For example, the weather forecast published to the weather website is a service because the information concludes an interaction between the service provider (the weather website) and the client (the website visitor). The interaction is concluded because the client obtains the weather forecast as a final output.
- How frequently is the information or data produced?
    - For information to be considered a service, the final output must be produced frequently or repeatedly. The more frequently the information or data is produced, the greater the likelihood that it is a service.
- How great is the need for the information?
    - The greater the recipient's need for the information, the greater the likelihood that the provision of it is a service. Consider whether access to the information helps ensure the well-being, health and safety of Canadians or economic viability of businesses and whether the lack of access to it could hinder this. For example, travel advisories or food recall warnings published to the Internet are services.
- Is there a timeliness factor associated with the need?
    - The greater the need for the information in a specified time frame, the greater the likelihood that it is a service. For example, consider weather services. The weather website publishes

information about the weather forecast with a high degree of frequency. Contrast this to a report or document that is published on the website only once a year.

- How many individuals or organizations access the information or data?
  - The greater the number of individuals that access the information or data as a final output, the greater the likelihood that it is a service. Given the wide range of services offered by the federal government, it is impossible to establish a threshold number because that number depends highly on the nature of the service and the operational context.

- Does the provision of information or data contribute directly to the achievement of an outcome?

  - Answering yes to this question increases the likelihood that the provision of the information or data is a service. For example, a call centre agent providing information or advice in the form of a final output contributes directly to an outcome; the client has obtained customized information and advice needed to access government programs and services.

B.1.7 Other examples of services

- Responses to access to information requests are considered as a service for all departments and agencies that process such requests. Note that the Office of the Privacy Commissioner of Canada is an oversight body that addresses *Privacy Act* complaints; it is not responsible for managing the intake process of ATIP requests on behalf of other institutions. Although requests may be submitted through an online portal, responses are managed and provided by departments and agencies to which the request is related.
- Call centres are considered a service because clients and Canadians make millions of calls to the government every year to get the information they need to make time-sensitive, important decisions.
- Public and media enquiries are considered as external services. The services result in a final output to the recipient/client, there are more than one recipient/client, the final output is produced repeatedly and the final output contributes to the achievement of an outcome.

B.1.8 Service owner vs. service provider

The activities that make up a service may be completed by one or several departments, including third-party organizations. When that is the case, it is especially important to understand the concept of service owner.

A service owner may differ from a service provider. A service owner is the organization that has the authority to offer the service. That authority is often conferred through legislation or through a regulatory or other instrument, and accountability is delegated to the appropriate level of manager.

B.2 Service management

Service management is the set of activities and practices undertaken by those responsible for designing, implementing, delivering, monitoring and continually improving the services for which they are accountable.

Effective service management enables excellence in the design and delivery of services. It also contributes to the achievement of public policy goals, delivers value for money, produces high levels of client satisfaction, and promotes confidence in government.

All individuals, businesses and organizations in Canada require services from the federal government at one time or another. They expect those services to be of high quality, and they expect government to provide services that are client-centric.

Service management in the Government of Canada is governed through the *Policy on Service and Digital* and requires deputy heads to apply the policy in a manner that reflects the requirement of client-centricity:

- 4.2.1.1 Ensuring the development and delivery of client-centric service by design, including access, inclusion, accessibility, security, privacy, simplicity, and choice of official language.

The above considerations are complemented by the consideration of well-known drivers of client satisfaction:

- ease of access (clients have access to what they need when they need it)
- timeliness (clients are satisfied with the amount of time it took to receive the service)
- positive outcome (clients receive what they need or understand why they cannot obtain it)
- professionalism (knowledgeable, fair treatment, respectful, polite, invested in client needs)
- recent service experience (clients base their opinions based on their most recent service experience)

B.3 Service types

Two approaches are proposed to enable departments to identify the types of services they provide. These approaches can either be based on:

- the service recipient
- the service output

These two types of services are not mutually exclusive.

Service types based on the service recipient	Service types based on the service output
1. External services	19 service types as identified in the Canadian Governments Reference Model (CGRM)
2. Internal services	
• Internal to departments	
• Interdepartmental	
• Internal Enterprise	

B.3.1 Service types based on the service recipient

When identifying service types based on the service recipient, services can be either external or internal to the government, as follows:

1. **External services**

An external service can be defined as a service where the intended recipient is a client that is external to the Government of Canada. The following are examples of external services:

- providing employment insurance services
- providing visitor access to a national park
- issuing a passport
- providing a permit for food products to indicate that they are safe for consumption

2. **Internal services**

Internal Services are groups of related activities and resources that the Government of Canada considers to be services in support of programs or required to meet corporate obligations of an organization. For a more detailed listing of service groupings included in internal services, consult Appendix B of the *Guide on Recording and Reporting of Internal Services Expenditures*.

Internal services can be grouped under 10 distinct service categories that support program delivery, regardless of the internal services delivery model in a department, as identified in the table below.

Internal service types	Examples
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
6. Information technology services	• Distributed computing • Application and database development and maintenance • Production and operations computing • Telecommunications network (data and voice)

Internal service types	Examples
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
	• IT security • IT program management
7. Legal services	• Legal advisory services • Litigation services

Internal service types	Examples
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
	• Legislative and regulatory drafting services
8. Management and oversight services	• Strategic policy and planning and government relations • Corporate policy, standards and guidelines • Investment planning

Internal service types	**Examples**
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
	• Departmental project management and oversight • Risk management • Performance and reporting • Internal audit

Internal service types	Examples
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
	• Evaluation • Parliamentary affairs • Access to information and privacy (ATIP) processing and reporting

Internal service types	Examples
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
9. Materiel management services	• Materiel planning • Use and maintenance of materiel • Disposal • Policy and procedures

Internal service types	Examples
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
10. Real property services	• Office fit-up • Office maintenance • Policy and procedures • Accommodation services

Internal service types	**Examples**
1. Acquisition services	• Procurement processing • Contract management • Monitoring and reporting • Policy and procedures
2. Communications services	• Public opinion research • Corporate identity • Managing public consultations • Managing media relations • Advertising, fairs and exhibitions for the entire department • Strategic communications and advice • Publishing
3. Financial management services	• Financial planning and budgeting • Corporate accounting • Expenditure control • Payments • Collections and receivables • Accounting for assets and liability
4. Human resources management services	• Human resources planning and reporting • Organization design • Job and position management • Employee staffing and orientation • Total compensation • Employee performance, learning, development and recognition • Permanent and temporary separations • Workplace management and labour relations • Human resources systems • Executive services
5. Information management services	• Data management services • Records and document management services • Library services • Web content management services • Archival services • Business intelligence and decision support services • Information management program management
	• Physical security

Internal services can be internal to a department, involve multiple departments, and be an internal enterprise type.

Internal to a department

Internal services are administered by a department to support its other programs and corporate obligations, regardless of where they are delivered in the department. These services enable the efficient and effective delivery of a department's mandate and programs.

Interdepartmental

An interdepartmental service generally involves two or more departments in the delivery of a service. Examples are:

- service agreements between departments and their portfolio organizations
- service agreements between two or more departments

Internal enterprise

An internal enterprise service can be defined as a service provided by a Government of Canada department to other federal departments on a government-wide basis. Internal enterprise services may be available for use by several departments or by all departments. The following are considered internal enterprise services:

- mandatory services, including those that are outsourced (for example, pay and pension services delivered by Public Services and Procurement Canada)
- shared or optional services, including those that are outsourced where the intent is to deliver them on a government-wide basis (for example, Shared Services Canada's email and network services)

B.3.2 Service types based on the service output

The Canadian Governments Reference Model (CGRM) provides a comprehensive overview of all Government of Canada service activity types. It identifies 19 service types based on the service output types and provides a set of target definitions that reflect common elements that may be considered when there are no established definition in place.

Departments are encouraged to refer to the 19 types of services when identifying and categorizing their services, as outlined in the table below.

Government of Canada Service Output Types

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
1	Funds; an amount of money	Services that acquire or dispense money	• Fixed (standard terms) contribution (for example, fee collection) • Fixed grant (non-repayable) • Variable contribution (for example, tax collection) • Variable grant • Emergency fixed contribution • Emergency fixed grant • Emergency variable contribution • Emergency variable grant	• Employment Insurance (EI) Benefits, Employment and Social Development Canada • Environmental Funding, Community Interaction Program, Environment and Climate Change Canada • Canada Student Grants and Canada Student Loans, Employment and Social Development Canada
2	Resources; a unit of resource	• Services that acquire or dispense units of resources or periods of use of a resource. • Includes labour, energy, land, facilities, movable assets and supplies, but excludes funds, information and rules (the latter are treated as distinct types of output [services]).	• Emergency consumable (for example, drugs) • Equipment for use (for example, computers) • Period of scheduled labour • Period of unscheduled labour • Provide immediate standard revocable tracked resource from stock • Routine consumable (for example, water supply)	• Workplace Technology Devices Provisioning, Shared Services Canada • Videoconferencing, Shared Services Canada • Aircraft parking, Transport Canada

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
			• Space for disposal (for example, land for sale) • Space for use (for example, rented building for accommodations)	
3	New knowledge (can also be called intellectual property)	Services that conduct research and produce information that was not known or derivable through computation or procedural means	No subtypes identified to date	• Labour market information, Employment and Social Development Canada • Research and testing on vehicles and child car seats, Transport Canada • Tides, Currents and Water Levels (CHS), Fisheries and Oceans Canada
4	Care and rehabilitation encounters; a care and rehabilitation encounter	Services that provide social or medical care or rehabilitation to people or that repair, upgrade, maintain or renovate property and natural features	• Response to an emergency care or rehabilitation requirement • Response to a non-emergency care or rehabilitation requirement	• Rehabilitation Services and Vocational Assistance Program, Veterans Affairs Canada • Clinical Care, Direct Service Delivery, Indigenous Services Canada • Architecture and Engineering, Public Services and Procurement Canada
5	Educational and training encounters; an educational and training encounter	Services that provide educational and training experiences to people	• Pre-designed repeatable education or training course • Custom education or training designed at time of request	• Learning Services, Canada School of Public Service • Cadets and Junior Canadian Rangers, National Defence • Aircraft Operations and Maintenance Training, Transport Canada
6	Recreational and cultural encounters; a recreational and cultural encounter	Services that provide experiences of a recreational or cultural nature to people	• Pre-designed repeatable recreational or cultural encounter • Recreational or cultural encounter designed at time of request	• Access to Parks Canada's places, Parks Canada • Access to cultural activities, The National Battlefields Commission • Military history and heritage, National Defence

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
7	Movements; a movement of a person or resource	• Services that move people and resources from point to point (includes energy, movable assets, supplies, funds, information) • At one extreme, energy, materials and people are moved, while at another extreme, information in the form of letters, email and messages are moved.	• Scheduled transport and standard route (for example, subway service, pipeline) • Scheduled transport and custom route (for example, limousine service, postal service, email service) • Scheduled custom transport and route (for example, military transport service, shipping service) • Immediate standard transport and custom route (for example, own vehicle) • Immediate custom transport and custom route	• Public ports, utilities and other services, Transport Canada • Flight Operations, Transport Canada
8	Advisory encounters; an advisory encounter (also known as an information encounter)	• Services that provide an encounter during which data, information or advice is conveyed to a party or a system • At one extreme, a lawyer advises a recipient, while at another extreme, a recipient acquires information from an online database, publication, etc.	• A standard advisory encounter is any advisory encounter where information is supplied from a database or through a prescriptive (computational, finite) analysis (either self-determined by the recipient or determined by the provider). • A custom advisory encounter is one	• Access to Information and Privacy, Department of Finance Canada • Crime Prevention Inventory, Public Safety, Public Safety Canada • Provision of distress and safety communications, Fisheries and Oceans Canada • Marine program weather services, Environment and Climate Change Canada • Labour market information, Employment and Social Development Canada • Ministerial correspondence (government-wide)

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
			where information is supplied after a skilled but non-prescriptive analysis of the recipient's requirements.	
9	Matches, referrals and linkages; a match, referral or linkage	Services that match, refer or link one party (requestor) to another party (responder) and in which the provider has an explicit or implicit duty to both parties in the match	• Prescriptive (computational) match between a requestor and known and finite range of responders • Non-prescriptive match between a requestor and an unknown or partially known range of responders may require locating additional responders as part of service delivery	• Job bank for employers, Employment and Social Development Canada • Job Bank: Find a Job, Employment and Social Development Canada • Employee Assistance Services, Health Canada • Clean Growth Hub, Innovation, Science and Economic Development Canada
10	Advocacy and promotional encounters; an advocacy or promotional encounter	Services that advocate or argue for positions or market government policies, programs and services by influencing, persuading or increasing awareness in people	• Pre-designed repeated encounter, such as courtroom arguments or media exposures • Encounters designed at time of request or delivery, such as direct persuasion	• Processing landowner complaints, National Energy Board • Orders-in-council, Privy Council Office • International trade and investment, Global Affairs Canada
11	Periods of agreement; a period of agreement	Services that resolve disputes or create agreements between parties	• Response in dispute resolution in potentially harmful circumstances • Routine response, for example, in agreement renewals	• Occupational Health and Safety Tribunal Canada, Employment and Social Development Canada • Review and appeal hearings, Veterans Review and Appeal Board.

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
12	Periods of permission; a period of permission granted by an authority	Services that express government authority by granting permission for a period of time to engage in activities, possess or control property or resources, or hold status, authority or privileges	• Recognition of revocable privileges or status, for example, pilot's licence, landed immigrant, heritage site • Recognition of inalienable rights, for example, citizenship and marital status • Immediate permission granting special powers, for example, deputizing • Immediate permission for an irreversible action, for example, search warrant	• Licensing for pilots and personnel, Transport Canada • Regular passport, Immigration, Refugees and Citizenship Canada • Temporary Resident Visa (TRV), Immigration, Refugees and Citizenship Canada • Issuance of permits, Parks Canada • Permits for trade in protected species, Environment and Climate Change Canada • Migratory game bird-hunting permits, Environment and Climate Change Canada
13	Findings; a finding	Services that inspect, investigate and analyze to uncover information and prepare findings and recommendations consistent with criteria and constraints such as the law, policy, approved standards and guidelines, etc., or consistent with credible opinion	• Repeatable and periodic finding following a prescribed procedure, purchase recommendation • Finding prepared to a specified requirement, for example, crime investigation	• FINTRAC policy interpretations, Financial Transactions and Reports Analysis Centre of Canada
14	Rulings and judgments; a ruling or judgment	Services that apply rules and dispense impartial decisions	A routine ruling, for example, a scheduled court case	• Income tax rulings, Canada Revenue Agency • Advance rulings and national customs rulings, Canada Border Services Agency • Review and appeal hearings, Veterans Review and Appeal Board

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
15	Penalties and periods of sanction; a penalty or period of sanction	Services that sanction, force compliance, mete out punishment and apply penalties	• Standard predetermined penalty, for example, a fine, dismissal • Penalty determined according to criteria or specification, for example, a prison sentence • Non-revocable standard sanction, for example, loss of citizenship • Non-revocable custom sanction, for example, provisional duty imposed following a Special Import Measures Act Decision	• Canadian sanctions, Global Affairs Canada • Pre-removal risk assessment, Immigration, Refugees and Citizenship Canada
16	Periods of protection; a period of protection	• Services that guard people and resources, including land, facilities, movable assets, supplies, funds and information, from threats • This service type provides proactive protection through monitoring, warning, guarding, storing, eliminating threats and reducing risks • Protection is provided in the form of surveillance and guarding of people and property against real or perceived risk,	• Scheduled guarding of standard threats to people or property, for example, building security • Scheduled guarding tailored to specific threats, for example, police escort, email spam prevention • Emergency guarding against standard threats, for example, fire alarm • Emergency guarding against known and unknown threats, for example,	• Law enforcement, Parks Canada • Classified infrastructure, Shared Services Canada

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
		violence, crime, accidents, and natural or synthetic hazards, and includes the stewardship measures necessary to ensure its continuance	quarantine order, curfew	
17	Interventions; an intervention	• Services that intervene, respond to threats and emergencies, give aid, and restore order • This service type provides reactive protection, which is delivered in the form of an alleviating response to a specific request for assistance for people or property experiencing real or potential risk, violence, accidents, and natural or synthetic hazards, and includes the stewardship measures necessary to ensure its continuance	• Pre-defined intervention, for example, fire suppression • Intervention designed to specific requirement, for example, military intervention	• Federal leadership on the Passenger Protect Program, Public Safety Canada • CANUTEC, Canadian Transport Emergency Centre, Transport Canada

	Canadian Governments Reference Model service output type and unit of output	Canadian Governments Reference Model service type description	Examples	Examples of Government of Canada services
18	Rules (laws, regulations, policies, strategies, plans, designs, standards); a rule	• Services that create or amend laws, regulations, policies, strategies, standards, plans and designs	• Regular rule-making, for example, a law, a policy, a plan • Emergency rule-making, for example, emergency measures or actions	• Regulatory development under the *First Nations Commercial and Industrial Development Act*, Crown-Indigenous Relations and Northern Affairs • Environmental assessment done by review panels, Canadian Environmental Assessment Agency • Rule-making, Canadian Transportation Agency • Emergency management exercises, Public Safety Canada • Emergency response assistance plans, Transport Canada
19	Implemented changes; an implemented change may also be called a project	Services that create new or elicit changes to existing organizations, programs, services, practices, systems and property	n/a	• Law Enforcement and Policing Research Unit, Public Safety Canada • Workplace solutions, Public Services and Procurement Canada

Appendix C: Information and data

Comparing the terms

The relationship between information and data can be expressed in a range of ways. Some practitioners use the two terms interchangeably, while others view information as being a part or constituent of data (or vice versa). While the *Policy on Service and Digital* supports the integrated management of information and data (along with cyber security, service delivery and IT), the two terms are intended to be conceptually and practically distinct. (See Appendix A of the *Policy on Service and Digital* for formal definitions of information and data.)

Data refers to quantitative, qualitative or other types of digitally mediated representations that are collected or created either automatically (for example, in the case of sensors) or through manual human labour (for example, data entry into a database or Excel spreadsheet). As descriptive representations, data generally correspond to factual entities, although the degree of their objectivity can vary significantly. What distinguishes data – structured, unstructured or otherwise – from information is that it has not undergone evaluation (for example, to assess its fitness for use), cleansing (for example, to ensure that there is only one value for each Canadian province or territory), been processed, or analyzed. As a result, the value of "raw" and unorganized data to a consumer tends to be relatively low because it does not convey the appropriate context and meaning needed for informed decision-making.

In contrast, information is meaningful data placed within its appropriate context. Data, once processed, structured and contextualized, is information. It is the result of an active process of preparing and analyzing data to help answer a question or support a particular objective such as the provision of a service. In other words, information can be described as actionable data. Even though it can be used by consumers or decision-makers, information is not necessarily of high quality. Moreover, whereas written text (for example, reports, briefings) has traditionally been viewed as information, the rise of techniques such as natural language processing has transformed it into a form of unstructured data. Having been evaluated, processed and/or analyzed, information can be used to inform policy and programming, as well as support the provision of services to citizens and businesses.

The definitions used by the European Commission for information and data summarize the relationship described so far. Data is defined as "concrete objective facts, measurements or observations that need to be processed to generate information." Information, on the other hand, "can be generated when data is categorised, analysed, interpreted, summarised and placed in context that gives it structure and meaning." To take an example, the individual responses of a sample of public servants to a survey question about the extent of their satisfaction with their workspaces represent data points. Yet to conclude that the percentage of public servants who are highly satisfied with their workspaces has increased by 35% when compared with the results of last year's survey represents information derived from these (and other) data points.

Based on the distinction outlined in this section, departments are advised to distinguish between the management of data and the management of information. While they are not to be understood as mutually exclusive, their varying life cycles demand distinct practices.

Information and data management governance and responsibilities

While data management and information management practices and considerations may be functionally distinct, the governance around both should be integrated. The *Policy on Service and Digital* (requirement 4.1.3.1) requires that deputy heads establish integrated governance for the management of information and data, as well as for service, IT and cyber security. Furthermore, the departmental CIO is clearly tasked with leading the departmental information **and** data management functions (as outlined in policy requirement 4.1.3.2). That being said, some deputy heads have designated chief data officers to carry out the data management function in practice. While the *Policy on Service and Digital* does not preclude such a case, it specifies that the departmental CIO is ultimately accountable for information and data management.

This responsibility is also linked to requirement 4.3.2.3 of the *Policy on Service and Digital*, which states that the deputy head must ensure that departmental responsibilities and accountability structures are clearly defined for the management of information and data. This could mean designating a single official (for example, the CIO) as responsible for both information and data management, or designating a chief data officer or another official with specific responsibility for data management. See subsection 1.2 of this guideline for more information on the designation of officials.

Appendix D: Identifying and Recognizing Information and Data of Business Value

Information and data of business value is defined in the Government of Canada (as outlined in the *Directive on Recordkeeping*) as “published and unpublished materials, regardless of medium or form, that are created or acquired because they enable and document decision-making in support of programs, services and ongoing operations, and support departmental reporting, performance and accountability requirements.” Any information and data that is not identified as having business value is considered transitory.

The distinction between information and data of business value and transitory information and data **is relevant** when it comes to:

- attaching metadata
- having authority to delete the information

The distinction between information and data of business value and transitory information and data **is not relevant** when it comes to:

- choosing a storage location
- assigning a security category
- protecting any personal information it contains
- responding to a request under the *Access to Information Act* or *Privacy Act*
- subjecting information and data to a litigation hold

As stated in the *Directive on Service and Digital*, it is the departmental CIO’s responsibility to identify information and data of business value in their organization. Refer to Guidance on Identifying Information of Business Value for more information. While many departments will have identified the same or similar information and data as having business value (for example, memoranda, briefing notes, records of decision), it is necessary to examine the specific functions and activities of the organization in order to arrive at an accurate listing of what has business value. It is then up to managers to inform employees of their duty to document activities and decisions of business value and employees to carry out that requirement in their daily work.

In order to ensure the ongoing value of these information and data resources of business value, capture them along with any relevant metadata (for example, subject, author, transmittal data) to ensure that they are complete, authentic and reliable. Retain information and data of business value in accordance with departmental records management standards and procedures, stored or profiled within a designated corporate repository, and protected against damage and loss.

The following are examples of the types of information and data that may have business value and which you might create, acquire or collect to document business functions and activities:

- transactions: orders, receipts, requests, confirmations
- interactions between clients, vendors, partners
- planning documents: budgets, forecasts, work plans, blueprints (technical or engineering designs), information architecture schematics
- reports, policy, briefing notes, memoranda, or other papers that support business activities: all significant versions (those that were circulated for comment or that contain comments related to the substance of the content and provide evidence of the document's evolution), the final product, distribution information
- meeting documents: agendas, official minutes, records of decision
- records of contact with lobbyists (in accordance with the *Lobbying Act*, which requires designated public office-holders to retain information about contact with lobbyists)
- committee documents: terms of reference, list of members
- form letters or templates used to collect responses, related instructions, completed responses in any format
- client records: applications, evaluations, emails, assessments
- records of discussions, deliberations or any situation related to any of the above that further documents the decisions made along with the logic used
- information and data resources that could provide additional information for auditing and monitoring activities and programs